

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
AUSTIN DIVISION

DEFENSE DISTRIBUTED and	§	Case No. 15-CV-372-RP
SECOND AMENDMENT FOUNDATION, INC.,	§	
	§	
Plaintiffs,	§	
	§	
v.	§	
	§	
U.S. DEPARTMENT OF STATE, et al.,	§	
	§	
Defendants.	§	
-----	§	

MEMORANDUM OF POINTS AND AUTHORITIES IN SUPPORT OF
PLAINTIFFS' MOTION FOR PRELIMINARY INJUNCTION

Come now Plaintiffs, Defense Distributed and Second Amendment Foundation, Inc., by and through counsel, and submit their Memorandum of Points and Authorities in Support of their Motion for Preliminary Injunction.

Dated: May 11, 2015

Respectfully submitted,

GURA & POSSESSKY, PLLC

FISH & RICHARDSON P.C.

Alan Gura
Virginia Bar No. 68842*
Gura & Possessky, PLLC
105 Oronoco Street, Suite 305
Alexandria, Virginia 22314
703.835.9085 / Fax 703.997.7665
alan@gurapossessky.com

/s/ William B. Mateja
William T. "Tommy" Jacks
Texas State Bar No. 10452000
William B. Mateja
Texas State Bar No. 13185350
David S. Morris
Texas State Bar No. 24032877
FISH & RICHARDSON P.C.
One Congress Plaza, Suite 810
111 Congress Avenue
Austin, Texas 78701
(512) 472-5070 (Telephone)
(512) 320-8935 (Facsimile)
jacks@fr.com
dmorris@fr.com
mateja@fr.com

Matthew Goldstein
D.C. Bar No. 975000*
Matthew A. Goldstein, PLLC
1012 14th Street NW, Suite 620
Washington, DC 20005
202.550.0040/Fax 202.683.6679
matthew@goldsteinpllc.com

Josh Blackman
Virginia Bar No. 78292*
1303 San Jacinto Street
Houston, Texas 77002
202.294.9003/Fax: 713.646.1766
joshblackman@gmail.com

*Admission pro hac vice pending

TABLE OF CONTENTS

Preliminary Statement.	1
Statement of Facts.	1
1. Defendants’ Regulation of “Technical Data”.	1
2. Defense Distributed’s Publication of Technical Data.	5
3. Defendants’ Imposition of a Prior Restraint Against Plaintiffs’ Speech.	7
a. The Published Files.	7
b. The “Ghost Gunner” Files.	8
c. The CAD Files.	8
d. Prior Restraint on Other Files.	9
4. Great, Irreparable, and Continuing Harm.	9
Summary of Argument.	10
Argument.	10
I. Plaintiffs Are Likely to Succeed on the Merits.	10
A. Congress Never Authorized Defendants’ Censorship of Privately-Generated, Unclassified Speech.	10
B. Defendants Are Violating Plaintiffs’ First Amendment Rights.	14
1. Plaintiffs’ Files Constitute Protected Speech.	14
2. ITAR’s Application to All Public, Unclassified Speech Containing Technical Data Is Unconstitutionally Overbroad.	16
3. Defendants Impose an Unconstitutional Prior Restraint Against Plaintiffs’ Lawful Speech.	19
a. Unbridled Discretion to Censor Speech.	20
b. Lengthy Delays and the Lack of Procedural Safeguards.	21

4.	Defendants’ Speech Regulation of Plaintiffs’ Speech Fails Any Level of First Amendment Scrutiny.	23
C.	Defendants’ Prior Restraint is Void for Vagueness.	24
D.	Defendants Are Violating Plaintiffs’ Second Amendment Rights.	25
1.	The Government Bears the Burden of Proving that Laws Burdening Second Amendment Rights Pass Heightened Scrutiny Review.	25
2.	The Second Amendment Secures the Right to Produce Firearms, and to Exchange Technical Data Concerning Firearms.	26
3.	Defendants’ Regulations Fail Any Level of Second Amendment Scrutiny.	28
II.	Defendants’ Licensing Scheme Irreparably Harms Plaintiffs.	29
III.	The Balance of Equities Favors Granting Injunctive Relief.	30
IV.	The Public Interest Warrants Injunctive Relief.	30
V.	No Bond or Other Security Is Required as a Condition of Providing Injunctive Relief.	30
	Conclusion.	30

TABLE OF AUTHORITIES

Cases

<i>Alexander v. United States</i> , 509 U.S. 544 (1993)	19
<i>Ashcroft v. Free Speech Coalition</i> , 535 U.S. 234 (2002)	15
<i>Awad v. Ziri</i> ax, 670 F.3d 1111 (10th Cir. 2012)	30
<i>Bernstein v. DOC</i> , No. C-95-0582-MHP, 2004 U.S. Dist. LEXIS 6672 (N.D. Cal. Apr. 19, 2004).	15
<i>Bernstein v. U.S. Dep’t of State</i> , 192 F.3d 1308 (9th Cir. 1999) (en banc)	15
<i>Bernstein v. U.S. Dep’t of State</i> , 922 F. Supp. 1426 (N.D. Cal. 1996).	15, 21
<i>Bernstein v. U.S. Dep’t of State</i> , 945 F. Supp. 1279 (N.D. Cal. 1996)	15
<i>Bernstein v. U.S. Dep’t of State</i> , 974 F. Supp. 1288 (N.D. Cal. 1997)	15
<i>Bernstein v. United States Dep’t of Justice</i> , 176 F.3d 1132 (9th Cir. 1999)	15
<i>Bowen v. Georgetown Univ. Hospital</i> , 488 U.S. 204 (1988)	10
<i>Burson v. Freeman</i> , 504 U.S. 191 (1992)	23
<i>Carey v. Pop. Servs. Int’l</i> , 431 U.S. 678 (1977)	27
<i>Catholic Leadership Coalition of Texas v. Reisman</i> , 764 F.3d 409 (5th Cir. 2014)	16, 19
<i>Chesapeake B & M, Inc. v. Harford County</i> , 58 F.3d 1005 (4th Cir. 1995)	20

<i>Chevron, U.S.A., Inc. v. Natural Res. Def. Council, Inc.</i> , 467 U.S. 837 (1984)	13
<i>Christensen v. Harris County</i> , 529 U.S. 576 (2000)	13, 14
<i>Citizens United v. FEC</i> , 558 U.S. 310 (2010)	23
<i>City of Lakewood v. Plain Dealer Publ’g Co.</i> , 486 U.S. 750 (1988)	20
<i>Connally v. General Const. Co.</i> , 269 U.S. 385 (1926)	24
<i>Deerfield Med. Center v. City of Deerfield Beach</i> , 661 F.2d 328 (5th Cir. 1981)	29
<i>District of Columbia v. Heller</i> , 554 U.S. 570 (2008)	25, 26, 29
<i>East Brooks Books, Inc. v. Shelby County</i> , 588 F.3d 360 (6th Cir. 2009)	20
<i>Elrod v. Burns</i> , 427 U.S. 347 (1976)	29
<i>Ezell v. City of Chicago</i> , 651 F.3d 684 (7th Cir. 2011)	27, 29
<i>Fantasy Ranch, Inc. v. City of Arlington</i> , 459 F.3d 546 (5th Cir. 2006)	21
<i>Forsyth County v. Nationalist Movement</i> , 505 U.S. 123 (1992)	20
<i>Freedman v. Maryland</i> , 380 U.S. 51 (1965)	16, 21, 22
<i>FW/PBS, Inc. v. Dallas</i> , 493 U.S. 215 (1990)	20
<i>Gibson v. Tex. Dep’t of Ins.–Div. of Workers’ Comp.</i> , 700 F.3d 227 (5th Cir. 2012)	19

<i>Gorin v. United States</i> , 312 U.S. 19 (1941)	17, 18
<i>Grayned v. City of Rockford</i> , 408 U.S. 104 (1972)	24
<i>Herceg v. Hustler Magazine, Inc.</i> , 814 F.2d 1017 (5th Cir. 1987)	15
<i>Hoechst Diafoil Co. v. Nan Ya Plastics Corp.</i> , 174 F.3d 411 (4th Cir. 1999)	30
<i>Holder v. Humanitarian Law Project</i> , 561 U.S. 1 (2010)	17
<i>Hynes v. Mayor & Council of Oradell</i> , 425 U.S. 610 (1976)	24
<i>Immigration and Naturalization Service v. St. Cyr</i> , 533 U.S. 289 (2001)	11
<i>Jackson Women’s Health Org. v. Currier</i> , 760 F.3d 448 (5th Cir. 2014)	30
<i>Junger v. Daily</i> , 209 F.3d 481 (6th Cir. 2000)	14
<i>Kaepa, Inc. v. Achilles Corp.</i> , 76 F.3d 624 (5th Cir. 1996)	30
<i>Louisiana Pub. Serv. Comm’n v. FCC</i> , 476 U.S. 355 (1986)	10
<i>Mance v. Holder</i> , No. 4:14-cv-539-O, 2015 U.S. Dist. LEXIS 16679 (N.D. Tex. Feb. 11, 2015)	27
<i>Marceaux v. Lafayette City-Parish Consol. Gov’t</i> , 731 F.3d 488 (5th Cir. 2013)	19
<i>Martin v. Harrington & Richardson, Inc.</i> , 743 F.2d 1200 (7th Cir. 1984)	26
<i>McCullen v. Coakley</i> , 134 S. Ct. 2518 (2014)	23

<i>Michigan v. EPA</i> , 268 F.3d 1075 (D.C. Cir. 2001).....	10
<i>Miller v. California</i> , 413 U.S. 15 (1973).....	14
<i>Nat’l Endowment for the Arts v. Finley</i> , 524 U.S. 569 (1998).....	24
<i>Nat’l Rifle Ass’n of Am., Inc. v. Bureau of Alcohol, Tobacco, Firearms & Explosives</i> , 700 F.3d 185 (5th Cir. 2012)	25, 26, 28
<i>Reliable Consultants, Inc. v. Earle</i> , 517 F.3d 738 (5th Cir. 2008).....	27
<i>Richmond Newspapers v. Virginia</i> , 448 U.S. 555 (1980).....	26
<i>Riley v. Nat’l Fed. of Blind of N.C.</i> , 487 U.S. 781 (1988).....	22
<i>Shuttlesworth v. Birmingham</i> , 394 U.S. 147 (1969).....	20
<i>Simon & Schuster, Inc. v. Members of the N.Y. State Crime Victims Bd.</i> , 502 U.S. 105 (1991)	23
<i>Skidmore v. Swift & Co.</i> , 323 U.S. 134 (1944).....	13, 14
<i>Speiser v. Randall</i> , 357 U.S. 513 (1958).....	16
<i>Texas v. Seatrain Int’l, S.A.</i> , 518 F.2d 175 (5th Cir. 1975)	10
<i>United States v. Alvarez</i> , 132 S. Ct. 2537 (2012).....	16
<i>United States v. Brown</i> , 218 F.3d 415 (5th Cir. 2000)	19
<i>United States v. Edler Industries</i> , 579 F.2d 516 (9th Cir. 1978).....	17-19

<i>United States v. Featherston</i> , 461 F.2d 1119 (5th Cir. 1972)	17
<i>United States v. Henry</i> , 688 F.3d 637 (9th Cir. 2012).....	27
<i>United States v. Marzzarella</i> , 614 F.3d 85 (3d Cir. 2010).	28
<i>United States v. Masciandaro</i> , 638 F.3d 458 (4th Cir. 2011)	28
<i>United States v. Mead Corp.</i> , 533 U.S. 218 (2001).....	13, 14
<i>United States v. Playboy Entm’t Group</i> , 529 U.S. 803 (2000)	23
<i>United States v. Scruggs</i> , 714 F.3d 258 (5th Cir. 2013)	16
<i>United States v. Stevens</i> , 559 U.S. 460 (2010).....	16, 23
<i>Universal City Studios, Inc. v. Corley</i> , 273 F.3d 429 (2d Cir. 2001).	14
<i>Winter v. Natural Res. Def. Council, Inc.</i> , 555 U.S. 7 (2008)	10
 Statutes, Rules and Regulations	
18 U.S.C. § 2339A(a).....	17
18 U.S.C. § 794(a).	17
22 C.F.R. Part 120 et seq.....	1
22 C.F.R. § 120.10.	21
22 C.F.R. § 120.10(a)(1).	2
22 C.F.R. § 120.10(b).....	2, 4, 7

22 C.F.R. § 120.11.	4, 7
22 C.F.R. § 120.11(a).	4
22 C.F.R. § 120.11(a)(7)	4
22 C.F.R. § 120.17(a)(1).	1
22 C.F.R. § 120.17(a)(4).	1, 12
22 C.F.R. § 120.4(a).	2, 21
22 C.F.R. § 120.41.	2
22 C.F.R. § 120.6	1, 21
22 C.F.R. § 121.1.	1, 21
22 C.F.R. § 121.1	2
22 C.F.R. § 125.4(b)(13).	3
22 C.F.R. § 128.1.	22
22 U.S.C. § 2778(a)(1).	1, 12
22 U.S.C. § 2778(c).	1
22 U.S.C. § 2778(e).	1
22 U.S.C. § 2778(h).	22
Fed. R. Civ. P. 65(c)	30

Other Authorities

49 Fed. Reg. 47,682 (December 6, 1984)	4, 13
74 Fed. Reg. 63497 (December 3, 2009).	22

Andy Greenberg, “3D-Printed Guns As Art: London Design Museum Buys Two ‘Liberator’ Printed Pistols,” <i>Forbes</i> , (Sep. 15, 2013), www.forbes.com/sites/andygreenberg/2013/09/15/3d-printed-guns-as-art-london-design-museum-buys-two-liberator-printed-pistols (last visited May 4, 2015).....	6
Chris Anderson, “The New MakerBot Replicator Might Just Change Your World,” <i>Wired</i> (Sep. 19, 2012) http://www.wired.com/2012/09/how-makerbots-replicator2-will-launch-era-of-desktop-manufacturing/all (last visited May 6, 2015).....	5
Eugene Volokh, <i>Crime-Facilitating Speech</i> , 57 <i>Stan. L. Rev.</i> 1095 (2005).....	15
Geoffrey Fowler, “MakerBot’s Bre Pettis: 3-D Printers Are for ‘Everyone,’” <i>Wall St. J. Blog</i> (June 18, 2014) http://blogs.wsj.com/personal-technology/2014/06/18/makerbots-bre-pettis-3-d-printers-are-for-everyone (last visited May 6, 2015).....	5
Mark Wilson, “Artist Warps 3-D Printed Gun Blueprints, Protests Gun Violence,” <i>Fast Company</i> (April 15, 2014), http://www.fastcodesign.com/3028300/infographic-of-the-day/artist-warps-3-d-printed-gun-blueprints-protests-gun-violence (last visited May 5, 2015).....	6
Paola Antonelli, “Design and Violence Debate I: Open Source,” <i>MOMA</i> (March 27, 2014) http://designandviolence.moma.org/design-and-violence-debate-i-open-source (last visited May 4, 2015).....	6
Peter Jensen-Haxel, <i>3D Printers, Obsolete Firearm Supply Controls, and the Right to Build Self-Defense Weapons Under Heller</i> , 42 <i>Golden Gate U. L. Rev.</i> 447 (2012).	27
Rachel Donadio, “A History of the Now, Found in Politically Charged Objects,” <i>New York Times</i> (July 6, 2014) http://www.nytimes.com/2014/07/07/arts/design/victoria-and-albert-museum-pushes-boundaries-of-collecting.html (last visited May 4, 2015).....	6
The Writings of Thomas Jefferson (T.J. Randolph, ed., 1830).	27
“Final Commodity Jurisdiction Determinations,” https://www.pmdtc.state.gov/commodity_jurisdiction/determination.html (last visited May 8, 2015).	2

MEMORANDUM OF POINTS AND AUTHORITIES IN SUPPORT OF
PLAINTIFFS' MOTION FOR PRELIMINARY INJUNCTION

PRELIMINARY STATEMENT

Contrary to the Justice Department's advice, and in derogation of rulemaking specifically designed to prevent such conduct, Defendants impose an unconstitutional prior restraint against Plaintiffs' lawful speech. By asserting that Internet postings regarding arms of the kind in common civilian use for traditional lawful purposes constitute "exports" subject to prepublication approval license requirements under the International Traffic in Arms Regulations (22 C.F.R. Part 120 et seq.) ("ITAR"), Defendants plainly violate Plaintiffs' First, Second, and Fifth Amendment rights, and those of their customers, visitors and members. A preliminary injunction is warranted.

STATEMENT OF FACTS

1. *Defendants' Regulation of "Technical Data"*

The State Department's Directorate of Defense Trade Controls ("DDTC") administers the ITAR regime in order to effectuate the President's limited control over the export of "defense articles" under the Arms Export Control Act of 1976 ("AECA"), 22 U.S.C. § 2778(a)(1). ITAR's "U.S. Munitions List" ("USML"), 22 C.F.R. § 121.1, describes those "defense articles" whose export requires advance government authorization—including "technical data," 22 C.F.R. § 120.6. "Export means," inter alia, "[s]ending or taking a defense article out of the United States in any manner, except by mere travel outside of the United States by a person whose personal knowledge includes technical data," 22 C.F.R. § 120.17(a)(1), and "[d]isclosing (including oral or visual disclosure) or transferring technical data to a foreign person, whether in the United States or abroad," 22 C.F.R. § 120.17(a)(4). Unauthorized exports are punishable by up to twenty years in prison, fines of up to \$1,000,000, and civil penalties up to \$500,000. 22 U.S.C. § 2778(c), (e).

The ITAR's USML purports to cover twenty-one categories of "technical data," broadly defined as information "required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance or modification of defense articles." 22 C.F.R. § 120.10(a)(1). This includes "information in the form of blueprints, drawings, photographs, plans, instructions or documentation" and "software" "directly related to defense articles," *Id.*, although it excludes, *inter alia*, "general scientific, mathematical, or engineering principles commonly taught in schools, colleges, and universities, or information in the public domain" 22 C.F.R. § 120.10(b). When referring to various types of "technical data," the USML utilizes additional vague terms, such as "military application," *see, e.g.*, 22 C.F.R. § 121.1 at USML paragraphs XII(b), XV(c), and XVIII(b), which is undefined; and/or "specially designed," whose definition exceeds 900 words, 22 C.F.R. § 120.41. Moreover, the USML's Category XXI is a catch-all provision, controlling "Articles, Technical Data, and Defense Services Not Otherwise Enumerated." 22 C.F.R. § 121.1 at USML paragraph XXI(a). These problems in interpreting the scope of ITAR control are aggravated by the fact that, since 2011, the ITAR has been the subject of over fifty proposed and final published notices of rulemaking in the Federal Register.

"[I]f doubt exists as to whether an article or service is covered by the U.S. Munitions List," prospective exporters must obtain a "commodity jurisdiction" determination from DDTC. 22 C.F.R. § 120.4(a). DDTC reports that over four thousand commodity jurisdiction requests have been submitted since 2010.¹ Defendants identify the Office of Freedom of Information and Security Review, the predecessor to the Department of Defense Office of Prepublication Review and Security ("DOPSR"), as the government agency from which persons must obtain prior approval before they

¹"Final Commodity Jurisdiction Determinations," https://www.pmddtc.state.gov/commodity_jurisdiction/determination.html (last visited May 8, 2015).

can publish unclassified technical information subject to ITAR control, regardless of whether the information is privately created. 22 C.F.R. § 125.4(b)(13). However, neither the Code of Federal Regulations nor any other public law establishes a timeline for decision, standard of review, or an appeals process for DOPSR public release determinations. Worsening this situation, DOPSR refuses to review information that it deems is not clearly subject to the ITAR without a formal commodity jurisdiction determination.

Obtaining a commodity jurisdiction determination can take a long time. Reportedly, nonpublic National Security Council (“NSC”) guidelines establish a sixty-day deadline for DDTC to render a commodity jurisdiction determination. App. 17. But Government Accountability Office, Office of Inspector General and Defendant DDTC’s reports show that the NSC guidelines are routinely disregarded, as commodity jurisdiction requests languish at DDTC awaiting final determinations for well over a year or more. App. 36-41, 84-86.

From 1969 to 1984, Footnote 3 to former ITAR Section 125.11 implied a prepublication approval requirement on privately generated, ITAR-controlled technical data, stating that “[t]he burden for obtaining appropriate U.S. Government approval for the publication of technical data falling within the definition in § 125.01, including such data as may be developed under other than U.S. Government contract, is on the person or company seeking publication.” App. 200. Beginning in 1978, the U.S. Department of Justice’s Office of Legal Counsel issued a series of publicly-available opinions advising Congress, the White House, and the State Department that the use of ITAR to impose a prior restraint on publications of privately generated unclassified information violates the First Amendment. App. 99-196.

In 1980, Defendant DDTC’s predecessor, the Department of State Office of Munitions Control, issued official guidance providing that “[a]pproval is not required for publication of data

within the United States as described in Section 125.11(a)(1). Footnote 3 to Section 125.11 does not establish a prepublication review requirement.” App. 205. Thereafter, the State Department removed Footnote 3 from ITAR, expressly stating its intent to address First Amendment concerns. *See* 49 Fed. Reg. 47,682, 47,683 (December 6, 1984) (“Concerns were expressed, for example, on licensing requirements as they relate to the First Amendment to the Constitution. The revision seeks to reflect these concerns . . .”). As such, to the extent ITAR imposed any prepublication approval requirement on public speech containing unclassified technical information, the requirement was ostensibly removed in 1984.

Moreover, as noted *supra*, ITAR now expressly excludes from its scope information found in the public domain. *See* 22 C.F.R. § 120.10(b). A reasonable person reading ITAR’s expansive definition of “public domain,” 22 C.F.R. § 120.11, would conclude that private speech can thus enter the public domain without U.S. government approval. This is especially so considering that “public release . . . after approval by the cognizant U.S. government department or agency,” 22 C.F.R. § 120.11(a)(7) is but one of eight sources of “information which is published and which is generally accessible or available to the public,” 22 C.F.R. § 120.11(a). Moreover, anyone reading the ITAR would reason that “cognizant U.S. government department of agency” is only relevant to information generated under government contracts, and not to privately generated information.

The Internet contains a large, ever-expanding array of technical information arguably subject to ITAR control. Simple Google, Amazon, and Yahoo searches reveal all manner of technical data that might well fit within one or another USML designation published in books, journals, and other mediums. Indeed, in 1997, the Department of Justice reported to Congress that

[i]t is readily apparent from our cursory examination that anyone interested in manufacturing a bomb, dangerous weapon or weapon of mass destruction can easily obtain detailed instructions for fabricating and using such a device. Available sources include not

only publications from the so-called underground press but also manuals written for legitimate purposes, such as military, agricultural, industrial and engineering purposes. Such information is also readily available to anyone with access to a home computer equipped with a modem.

App. 160.

2. *Defense Distributed's Publication of Technical Data*

First developed in the 1980s, three-dimensional (“3D”) printing technology allows a computer to “print” a physical object (as opposed to a two-dimensional image on paper). This technology was not widely available until open source communities such as the RepRap Project (www.reprap.org)² developed inexpensive but capable 3D printers.³ Today, 3D printers are sold at stores such as Home Depot and Best Buy, and the instructions for printing everything from jewelry to toys to car parts are shared and exchanged freely online at sites like GrabCAD.com and Thingiverse.com.

Plaintiff Defense Distributed was organized and is operated for the purpose of defending the civil liberty of popular access to arms guaranteed by the United States Constitution through facilitating global access to, and the collaborative production of, information and knowledge related to the 3D printing of arms; and to publish and distribute, at no cost to the public, such information and knowledge on the Internet in promotion of the public interest. App. 1, ¶ 2. Beginning in 2012, Defense Distributed privately generated, and posted on the Internet for free access by the public,

²Open source communities are online forums through which individuals freely and collaboratively share their knowledge and discoveries.

³Geoffrey Fowler, “MakerBot’s Bre Pettis: 3-D Printers Are for ‘Everyone,’” *Wall St. J. Blog* (June 18, 2014) <http://blogs.wsj.com/personal-technology/2014/06/18/makerbots-bre-pettis-3-d-printers-are-for-everyone> (last visited May 6, 2015); Chris Anderson, “The New MakerBot Replicator Might Just Change Your World,” *Wired* (Sep. 19, 2012) <http://www.wired.com/2012/09/how-makerbots-replicator2-will-launch-era-of-desktop-manufacturing/all> (last visited May 6, 2015)

technical information about various gun-related items, including a trigger guard, grips, two receivers, a magazine for AR-15 rifles, and a handgun named “The Liberator” (the “Published Files”). At the time, there were no publicly known DDTC enforcement actions for the posting of files on the Internet. *Id.* ¶ 3.

The Published Files were downloaded hundreds of thousands of times. App. 2, ¶ 4. The Liberator files in particular generated national media attention, with coverage in Forbes, CNN, NBC News, the Wall Street Journal, and even an episode of The Colbert Report. *Id.* Apart from their functional aspects, the Published Files have also proven to have artistic and political utility. For example, one artist has repurposed the Liberator schematics to create a statement protesting gun violence.⁴ London’s Victoria & Albert Museum purchased two 3D printed Liberators to display during its ongoing Design Festival.⁵ And the Liberator prompted the Museum of Modern Art in New York to host a debate concerning the intersection of design and violence.⁶

⁴Mark Wilson, “Artist Warps 3-D Printed Gun Blueprints, Protests Gun Violence,” *Fast Company* (April 15, 2014), <http://www.fastcodesign.com/3028300/infographic-of-the-day/artist-warps-3-d-printed-gun-blueprints-protests-gun-violence> (last visited May 5, 2015).

⁵Andy Greenberg, “3D-Printed Guns As Art: London Design Museum Buys Two ‘Liberator’ Printed Pistols,” *Forbes*, (Sep. 15, 2013), www.forbes.com/sites/andygreenberg/2013/09/15/3d-printed-guns-as-art-london-design-museum-buys-two-liberator-printed-pistols (last visited May 4, 2015); Rachel Donadio, “A History of the Now, Found in Politically Charged Objects,” *New York Times* (July 6, 2014) <http://www.nytimes.com/2014/07/07/arts/design/victoria-and-albert-museum-pushes-boundaries-of-collecting.html> (last visited May 4, 2015).

⁶Paola Antonelli, “Design and Violence Debate I: Open Source,” *MOMA* (March 27, 2014) <http://designandviolence.moma.org/design-and-violence-debate-i-open-source> (last visited May 4, 2015).

3. *Defendants’ Imposition of a Prior Restraint Against Plaintiffs’ Speech*

a. *The Published Files*

On May 8, 2013, Defendant Smith, Chief of Defendant DDTC’s Enforcement Division, sent Defense Distributed a letter that warned:

DTCC/END is conducting a review of technical data made publicly available by Defense Distributed through its 3D printing website, DEFCAD.org, the majority of which appear to be related to items in Category I of the USML. Defense Distributed may have released ITAR-controlled technical data without the required prior authorization from the Directorate of Defense Trade Controls (DDTC), a violation of the ITAR . . . all such data should be removed from public access immediately.

App. 2, ¶ 5; App. 13-14.

At the time it posted the Published Files, Defense Distributed did not know that the Defendants would demand to pre-approve its speech. Defense Distributed believed, and continues to believe, that the United States Constitution guarantees a right to share truthful speech—especially speech concerning fundamental constitutional rights—in open forums. App. 2, ¶ 6. Moreover, as noted *supra*, ITAR specifically excludes from its coverage “technical data” appearing in the “public domain,” 22 C.F.R. § 120.10(b), the latter term appearing to broadly encompass Defense Distributed’s activities, *see* 22 C.F.R. § 120.11. Nevertheless, for fear of criminal and civil enforcement, Defense Distributed promptly complied with Defendants’ demands and removed all of the Published Files from its servers. App. 2, ¶ 6.

Defendants’ letter further directed Defense Distributed to submit the Published Files to DDTC for review using the “commodity jurisdiction” procedure. App. 2, ¶ 7, App. 14. Defense Distributed complied with Defendants’ request and filed ten (10) commodity jurisdiction requests covering the Published Files on June 21, 2013. App. 2, ¶ 7; Exh. 13. Nearly two years later, Defendants have still not responded to the requests. App. 2, ¶ 7.

b. *The “Ghost Gunner” Files*

On September 25, 2014, Defense Distributed requested DOPSR’s prepublication approval for public release of files containing technical information on a machine, named the “Ghost Gunner,” that can be used to manufacture a variety of items, including gun parts (the “Ghost Gunner Files”). App. 3, ¶ 8; Exh. 14.⁷ On October 1, 2014, DOPSR informed Defense Distributed this request for review was refused because DOPSR was unsure whether the Ghost Gunner was subject to ITAR. DOPSR further recommended that Defense Distributed submit another commodity jurisdiction request to the Defendants. App. 3, ¶ 8; Exh. 15.

Defense Distributed submitted another commodity jurisdiction request for the Ghost Gunner to Defendants on January 2, 2015. App. 3, ¶ 9; Exh. 16. On April 15, 2015, Defendant DDTC determined that the Ghost Gunner machine, user manual, and operating software are not subject to ITAR, but that “software, data files, project files, coding, and models for producing a defense article, to include 80% AR-15 lower receivers, are subject to the jurisdiction of the Department of State in accordance with [ITAR].” App. 3, ¶ 9; Exh. 17.

c. *The CAD Files.*

Since September 2, 2014, Defense Distributed has made multiple requests to DOPSR for prepublication review of certain computer-aided design (“CAD”) files. App. 3-4, ¶ 10; Exhs. 18-21. On December 31, 2014, nearly four months after the first such review request, DOPSR sent Defense Distributed two letters stating its refusal to review the CAD files. App. 4, ¶ 10; Exh. 22. The letters directed Defense Distributed to the DDTC Compliance and Enforcement Division for further

⁷Any milling machine can be modified to mill components that are unlawful to manufacture, just as any saw that may be purchased at a hardware store can be used to unlawfully shorten a shotgun. However, Ghost Gunner does not ship with the jigs and code to manufacture machine guns, and Defense Distributed has no intention of offering such items for sale. *Id.*

questions on public release of the CAD files. *Id.* However, because this is not the DDTC division responsible for issuing licenses or other DDTC authorizations, on January 5, 2015, Defense Distributed requested Defendants' guidance on how to obtain authorization from DDTC Compliance for release of the CAD files. To date, Defendants have not responded to Defense Distributed's request for guidance. App. 4, ¶ 11; Exh. 23.

d. *Prior Restraint on Other Files*

Defense Distributed has and will continue to create and possess other files that contain technical information, to include design drawings, rendered images, written manufacturing instructions, and other technical information that Defense Distributed intends to post to open forums on the Internet. Many of these files are described in the USML. App. 4, ¶ 13.

Plaintiff Second Amendment Foundation, Inc. ("SAF"), a non-profit membership organization, has over 650,000 members and supporters nationwide, including in Texas. The purposes of SAF include promoting the exercise of the right to keep and bear arms; and education, research, publishing and legal action focusing on the constitutional right to privately own and possess firearms, and the consequences of gun control. App. 6, ¶ 2. SAF's members have a keen interest in accessing, studying, sharing, modifying, and learning from Defense Distributed's various files, as well as similar 3D printing files related to firearm that they or other have created, but have been barred from doing so by Defendants' actions. *Id.* ¶ 3; App. 8, ¶ 4; App. 9, ¶ 5; App. 10, ¶ 4; App. 11, ¶ 5.

4. *Great, Irreparable, and Continuing Harm*

But for Defendants' impositions upon the distribution of the Published Files, Ghost Gunner Files, CAD Files, and Defense Distributed's other files (collectively, the "Subject Files"), Plaintiffs would freely distribute the Subject Files and other files relating to Second Amendment arms.

Plaintiffs refrain from distributing the Subject Files because they reasonably fear that Defendants would pursue criminal and civil enforcement proceedings against Plaintiffs for doing so. App. 4-5, ¶ 14; App. 7, ¶ 4. Defendants’ threats have thus silenced Plaintiffs. Defendants have deprived Plaintiffs’ customers, visitors and patrons of access to Plaintiffs’ speech; impeded their ability to likewise speak on the same subjects; and infringed their right to keep and bear arms.

SUMMARY OF ARGUMENT

“A plaintiff seeking a preliminary injunction must establish [1] that he is likely to succeed on the merits, [2] that he is likely to suffer irreparable harm in the absence of preliminary relief, [3] that the balance of equities tips in his favor, and [4] that an injunction is in the public interest.” *Winter v. Natural Res. Def. Council, Inc.*, 555 U.S. 7, 20 (2008) (citations omitted). These factors are measured along a “sliding scale . . . which takes into account the intensity of each [factor] in a given calculus.” *Texas v. Seatrain Int’l, S.A.*, 518 F.2d 175, 180 (5th Cir. 1975) (citation omitted). Each of these four factors weighs heavily in Plaintiffs’ favor.

ARGUMENT

I. PLAINTIFFS ARE LIKELY TO SUCCEED ON THE MERITS

A. CONGRESS NEVER AUTHORIZED DEFENDANTS’ CENSORSHIP OF PRIVATELY-GENERATED, UNCLASSIFIED SPEECH.

“It is axiomatic that an administrative agency’s power to promulgate legislative regulations is limited to the authority delegated by Congress.” *Bowen v. Georgetown Univ. Hospital*, 488 U.S. 204, 208 (1988). “[A]n agency literally has no power to act . . . unless and until Congress confers power upon it.” *Louisiana Pub. Serv. Comm’n v. FCC*, 476 U.S. 355, 374 (1986). Such authority “may not be lightly presumed.” *Michigan v. EPA*, 268 F.3d 1075, 1082 (D.C. Cir. 2001). And “when a particular interpretation of a statute invokes the outer limits of Congress’ power, we expect

a clear indication that Congress intended that result.” *Immigration and Naturalization Service v. St. Cyr*, 533 U.S. 289, 299 (2001) (citation omitted).

Defendants have aggrandized for themselves nothing less than a power to censor privately-generated, unclassified “technical data” on the Internet. Their apparent syllogism holds: (1) the Internet is available worldwide, and is also available to foreign persons within the United States; (2) all speech posted to the Internet is thus deemed “exported;” (3) the export of “technical data” may be licensed and reviewed under ITAR; therefore (4) all “technical data” posted to the Internet is subject to ITAR controls and procedures. Q.E.D. Before addressing the constitutionality of this breathtaking regulatory regime, the Court should ask whether Congress granted Defendants such authority. As the Justice Department and Defendants’ predecessors have opined, that question is answered “no.”

The only potential source of statutory authority for Defendants’ conduct would be found in the AECA, which authorizes the President, “[i]n furtherance of world peace and the security and foreign policy of the United States . . . to control the import and the export of defense articles and defense services and to provide foreign policy guidance to persons of the United States involved in the export and import of such articles and services.” 22 U.S.C. § 2778(a)(1). To this end, “[t]he President is authorized to designate those items which shall be considered as defense articles and defense services for the purposes of this section and to promulgate regulations for the import and export of such articles and services.” *Id.*

To be sure, Plaintiffs do not suggest that Defendants lack authority under the AECA to construct a narrowly-tailored regime to regulate the export of certain technical data. Nor do Plaintiffs suggest that uploading files to the Internet cannot be viewed, in some sense, as an export. Defendants can bar individuals from emailing classified blueprints for secret weapons systems to a foreign agent or providing technical assistance to a foreign person on designing defense articles. But

that is a very far cry from supposing that AECA authorizes the imposition of an indecipherable prior restraint against sharing *all* public speech containing “technical data” on the Internet. And were the AECA read to contain such a broad grant of prior restraint authority, there would be no reason to limit that authority to the Internet. Recall that Defendants have broadly defined “export” to encompass the act of “[d]isclosing (including oral or visual disclosure) . . . technical data to a foreign person . . . in the United States.” 22 C.F.R. § 120.17(a)(4). Any other publication of “technical data,” such as those appearing in countless scientific and academic publications, as well as on television and at the movies, would be subject to Defendants’ prior restraint. No American could stand on a street corner or public square of any town visited by foreign tourists and declaim “technical data” without being subject to Defendants’ prior restraint.

This is doubtless not what Congress had in mind when delegating authority to regulate the export of defense articles “[i]n furtherance of world peace and the security and foreign policy of the United States.” 22 U.S.C. § 2778(a)(1). In 1978, not long after the AECA’s enactment, the Justice Department doubted that the Act authorized a prior restraint against cryptographic speech, and warned, “It is by no means clear from the language or legislative history of either statute [AECA and ITAR] that Congress intended that the President regulate noncommercial dissemination of information, or considered the problems such regulation would engender.” App. 102.

[W]e wish to emphasize our doubts that the executive branch may validly provide for licensing or prior approval of exports of cryptographic information without more explicit Congressional authorization. The scope of the existing delegation of authority from Congress to the President, as we note above, is somewhat unclear. Before imposing a prior restraint on exports of public cryptographic information, we believe that a more clear cut indication of Congressional judgment concerning the need for such a measure is in order . . . further Congressional authorization would obviously be necessary in order to extend governmental controls to domestic as well as foreign disclosures of public cryptographic information.

App. 113 (citations omitted); *cf.* App. 115 (“we are uncertain whether the present legislative authority for the technical data provisions of ITAR is adequate.”)).

Defendants might claim that Congress’s statute is purposefully vague and indeterminate, leaving to them the task of creating regulations governing the export of defense articles—a task clothed with a fair degree of judicial deference under the rule of *Chevron, U.S.A., Inc. v. Natural Res. Def. Council, Inc.*, 467 U.S. 837, 842 (1984). But *Chevron* deference applies only “when it appears that Congress delegated authority to the agency generally to make rules carrying the force of law, and that the agency interpretation claiming deference was promulgated in the exercise of that authority.” *United States v. Mead Corp.*, 533 U.S. 218, 227-28 (2001). In other words, the agency action entitled to deference must involve the exercise of some delegated process. “[A]djudication or notice-and-comment rulemaking,” for example, may carry the force of law. *Id.* at 228. But “[i]nterpretations such as those in opinion letters—like interpretations contained in policy statements, agency manuals, and enforcement guidelines, all of which lack the force of law—do not warrant *Chevron*-style deference.” *Christensen v. Harris County*, 529 U.S. 576, 587 (2000) (citations omitted).

Defendants’ prior restraint scheme is plainly not the product of its duly adopted rules. To the contrary, as noted *supra*, First Amendment concerns prompted the State Department to withdraw the only ITAR provision potentially authorizing a prior restraint regime in 1984, 49 Fed. Reg. 47,682 (December 6, 1984), four years after advising that the offending provision “does not establish a prepublication review requirement.” App. 205. The prior restraint scheme has only been hinted at in Defendants’ threatening letter to Defense Distributed and, perhaps, in Defendants’ internal enforcement guidelines. “[I]nterpretations contained in formats such as opinion letters are ‘entitled to respect’ under our decision in *Skidmore v. Swift & Co.*, 323 U.S. 134, 140 (1944), but only to the

extent that those interpretations have the ‘power to persuade.’” *Christensen*, 529 U.S. at 587

(parallel and other citations omitted).

The weight [accorded to an administrative] judgment in a particular case will depend upon the thoroughness evident in its consideration, the validity of its reasoning, its consistency with earlier and later pronouncements, and all those factors which give it power to persuade, if lacking power to control.

Mead, 533 U.S. at 228.

Defendants’ prior restraint scheme plainly fails the *Skidmore* test. There is no evidence that Defendants, unlike their predecessors and the Department of Justice, ever properly considered the implications of applying a prior restraint to all speech containing technical data that might be accessed or overheard by a foreigner. The practice is also starkly inconsistent with earlier pronouncements, wherein the government took steps to clarify that export controls did *not* amount to a prior restraint on private speech. Nor has this prior restraint been consistently applied. Defense Distributed appears to be the scheme’s *only* target, other websites containing similar computer files are apparently unimpeded. App. 4, ¶ 12. Defendants’ actions in imposing a prior restraint on unclassified and public speech containing “technical data” lie beyond the authority delegated to them by Congress—assuming Congress could even restrict constitutional rights so broadly.

B. DEFENDANTS ARE VIOLATING PLAINTIFFS’ FIRST AMENDMENT RIGHTS.

1. *Plaintiffs’ Files Constitute Protected Speech.*

“The First Amendment protects works which, taken as a whole, have serious literary, artistic, political, or scientific value, regardless of whether the government or a majority of the people approve of the ideas these works represent.” *Miller v. California*, 413 U.S. 15, 34 (1973). “[C]omputer code conveying information is ‘speech’ within the meaning of the First Amendment” *Universal City Studios, Inc. v. Corley*, 273 F.3d 429, 449-50 (2d Cir. 2001); *see also Junger v.*

Daily, 209 F.3d 481, 485 (6th Cir. 2000) (“Because computer source code is an expressive means for the exchange of information and ideas about computer programming, we hold that it is protected by the First Amendment.”); *Bernstein v. United States Dep’t of Justice*, 176 F.3d 1132, 1141 (9th Cir.) (“*Bernstein IV*”) (“encryption software . . . must be viewed as expressive for First Amendment purposes, and thus is entitled to the protections of the prior restraint doctrine”), *reh’g in banc granted and opinion withdrawn*, 192 F.3d 1308 (9th Cir. 1999).⁸

To be sure, Plaintiffs’ speech might be used to facilitate crime,⁹ but that much is true of virtually all protected speech. “The prospect of crime . . . by itself does not justify laws suppressing protected speech.” *Ashcroft v. Free Speech Coalition*, 535 U.S. 234, 245 (2002).

The constitutional protection accorded to the freedom of speech and of the press is not based on the naive belief that speech can do no harm but on the confidence that the benefits society reaps from the free flow and exchange of ideas outweigh the costs society endures by receiving reprehensible or dangerous ideas.

Herceg v. Hustler Magazine, Inc., 814 F.2d 1017, 1019 (5th Cir. 1987). Thus, while speech may be regulated for its hazardous aspects, “first amendment protection is not eliminated simply because publication of an idea creates a potential hazard.” *Id.* at 1020. *See* Eugene Volokh, *Crime-Facilitating Speech*, 57 Stan. L. Rev. 1095, 1103 (2005).

⁸In *Bernstein v. U.S. Dep’t of State*, 922 F. Supp. 1426 (N.D. Cal. 1996) (“*Bernstein I*”), a district court held that the source code for an ITAR-designated cryptographic program constituted protected First Amendment expression. The court subsequently struck down ITAR in *Bernstein v. U.S. Dep’t of State*, 945 F. Supp. 1279 (N.D. Cal. 1996) (“*Bernstein II*”). When the government shifted control over the code’s export from the State Department to the Commerce Department, the plaintiff amended his complaint to challenge the relevant Export Administration Regulations. The court struck down these regulations as well, *Bernstein v. U.S. Dep’t of State*, 974 F. Supp. 1288 (N.D. Cal. 1997) (“*Bernstein III*”), and the Ninth Circuit affirmed that decision in *Bernstein IV*. Although the Court granted rehearing en banc, the government amended its regulations to exclude plaintiff’s code from export controls, mooting the case. *See Bernstein v. DOC*, No. C-95-0582-MHP, 2004 U.S. Dist. LEXIS 6672, at *6 & n.2 (N.D. Cal. Apr. 19, 2004).

⁹It is less obvious that Plaintiffs’ files would be particularly useful to foreign governments.

Furthermore, Defendants bear the burden of proving that Plaintiffs' speech is somehow unprotected. *See Freedman v. Maryland*, 380 U.S. 51, 58 (1965); *Speiser v. Randall*, 357 U.S. 513, 526 (1958). This they cannot do. This is not a case where the speech itself is inherently unprotected (e.g., perjury or fraud), or directly and exclusively aids and abets a criminal act. *Cf. United States v. Alvarez*, 132 S. Ct. 2537, 2547 (2012). Even were Plaintiffs' files purely functional and devoid of expressive content, Americans enjoy a fundamental right to possess the items described in and that can be created by the operation of Plaintiffs' files, which are legal to possess throughout most of the United States, including Texas.

2. *ITAR's Application to All Public, Unclassified Speech Containing Technical Data Is Unconstitutionally Overbroad.*

"A statute is overbroad if in banning unprotected speech, a substantial amount of protected speech is prohibited or chilled in the process." *United States v. Scruggs*, 714 F.3d 258, 267 (5th Cir. 2013) (quotation omitted). A speech restriction is unconstitutional if "no set of circumstances exists under which [the law] would be valid or . . . the statute lacks any plainly legitimate sweep." *Catholic Leadership Coalition of Texas v. Reisman*, 764 F.3d 409, 426 (5th Cir. 2014) (quoting *United States v. Stevens*, 559 U.S. 460, 472 (2010)). A restriction is also unconstitutionally overbroad if "a substantial number of [the law's] applications are unconstitutional, judged in relation to the statute's plainly legitimate sweep." *Id.* (quoting *Stevens*, 559 U.S. at 473).

Given Defendants' sweeping views of what constitutes an "export"—virtually all speech in the presence of foreigners, including all Internet speech—and their equally broad definition of "technical data," ITAR cannot withstand constitutional scrutiny.

Federal laws criminalizing speech typically require that the targeted speech be made with intent or knowledge that the information would be used to facilitate criminal conduct, or with

knowledge that a particular recipient of the information intends to use it in the furtherance of criminal activity. The Espionage Act, for example, only punishes those who seek to communicate “with intent or reason to believe that [the information] is to be used to the injury of the United States or to the advantage of a foreign nation.” 18 U.S.C. § 794(a); see *Gorin v. United States*, 312 U.S. 19, 28 (1941) (upholding constitutionality of Espionage Act owing to scienter requirement). And it is not a crime to provide material support or resources to terrorists, unless one “know[s] or intend[s] that they are to be used in preparation for, or in carrying out, a violation” of various law. 18 U.S.C. § 2339A(a); see *Holder v. Humanitarian Law Project*, 561 U.S. 1 (2010); see also *United States v. Featherston*, 461 F.2d 1119, 1121 (5th Cir. 1972) (upholding convictions for teaching the use or making of explosives or incendiary devices, as statute “requires those prosecuted to have acted with intent or knowledge that the information disseminated would be used in the furtherance of a civil disorder.”).

A scienter requirement should likewise limit ITAR’s reach in restricting speech. *United States v. Edler Industries*, 579 F.2d 516 (9th Cir. 1978). In *Edler*, the Ninth Circuit overturned a conviction under the AECA’s predecessor act, and the ITAR regulations then in effect, because the trial court rejected arguments that the technical data had non-military applications. The act and its

definition of technical data are susceptible of an overbroad interpretation. Their expansive language may be construed to restrict not only the export of arms and information directly leading to the production of articles on the Munitions List, but also the interchange of scientific and technical information that of itself is without any substantial military application.

Edler, 579 F.2d at 520. To avoid the constitutional problem, the court construed ITAR’s reach narrowly, to “control the conduct of assisting foreign enterprises to obtain military equipment and related technical expertise. So confined, the statute and regulations are not overbroad [or] an unconstitutional prior restraint on speech.” *Id.* at 521.

[T]echnical data must relate in a significant fashion to some item on the Munitions List. Moreover, adequate notice to the potential exporter requires that the relationship be clear . . . Presumably, Congress intended that the technical data subject to control would be directly relevant to the production of a specified article on the Munitions List, not simply vaguely useful for the manufacture of arms.

Id. at 520-21. “If the information could have both peaceful and military applications, as Edler contends that its technology does, the defendant must know or have reason to know that its information is intended for the prohibited use.” *Id.* at 521 (citing *Gorin*, 312 U.S. at 27-28).

Following *Edler*, the Department of Justice Office of Legal Counsel issued a memorandum to the State Department warning of “serious constitutional questions” were ITAR applied to “transactions in which an ‘exporter’ who is not otherwise connected or concerned with any foreign enterprise transmits technical data knowing, or having reason to know, that the data may be taken abroad and used by someone there in the manufacture or use of arms.” App. 121.

[T]he revised technical data provisions cannot constitutionally be applied to the dissemination of technical data by persons having no direct connection with foreign conduct in settings in which there is no more than belief or a reasonable basis for believing (1) that a foreign national may take the technical data abroad and (2) that the data could be used by someone there in the manufacture or use of items on the Munitions List.

App. 128. “For obvious reasons, the best legal solution for the overbreadth problem is for the Department of State, not the courts, to narrow the regulations.” App. 129; see also App. 131 (1981 DOJ Memorandum to Commerce Dep’t).

The Department of Justice reiterated these concerns in its 1997 report to Congress, counseling that prior restraints against Internet publication of bomb-making and use information violated the First Amendment, unless the publication was made “(i) with the intent that the information be used to facilitate criminal conduct, or (ii) with the knowledge that a particular recipient of the information intends to use it in furtherance of criminal activity.” App. 156.

Defendants' censorship disregards both of these limitations. Plaintiffs are not seeking to help foreigners build controlled weapons of war. Rather, they are merely communicating with their fellow Americans, through a website, information regarding simple arms of the kind in common use for traditional lawful purposes that are themselves constitutionally protected. Had Defense Distributed designed a new type of diesel engine, that engine's possible utility in a tank would not authorize the State Department to prohibit the dissemination of blue prints, CAD files, or even executable 3D printing files on automotive-themed websites. *Cf. Edler*, 579 F.2d at 519. There is simply no telling where Defendants' censorship might end, unless it ends here.

3. *Defendants Impose an Unconstitutional Prior Restraint Against Plaintiffs' Lawful Speech.*

"The classic prior restraint, of course, is an 'administrative [or] judicial order[] forbidding certain communications when issued in advance of the time that such communications are to occur.'" *Catholic Leadership Coalition*, 764 F.3d at 437 (quoting *Alexander v. United States*, 509 U.S. 544, 550 (1993) (other citations omitted)). Prior restraints are, "in other words, laws which require a speaker 'to obtain prior approval for any expressive activities.'" *Gibson v. Tex. Dep't of Ins.-Div. of Workers' Comp.*, 700 F.3d 227, 235 (5th Cir. 2012) (quoting *Alexander*, 509 U.S. at 550-51). "Prior restraints face a well-established presumption against their constitutionality." *Marceaux v. Lafayette City-Parish Consol. Gov't*, 731 F.3d 488, 493 (5th Cir. 2013) (quotation omitted).

In general, a prior restraint . . . will be upheld only if the government can establish that the activity restrained poses either a clear and present danger or a serious and imminent threat to a protected competing interest. The government must also establish that the order has been narrowly drawn and is the least restrictive means available.

United States v. Brown, 218 F.3d 415, 425 (5th Cir. 2000) (quotations omitted).

“Constitutional invalidity of prior restraints may result from one or both of ‘two evils . . . : (1) the risk of censorship associated with the vesting of unbridled discretion in government officials; and (2) ‘the risk of indefinitely suppressing permissible speech’ when a licensing law fails to provide for the prompt issuance of a license.” *East Brooks Books, Inc. v. Shelby County*, 588 F.3d 360, 369 (6th Cir. 2009) (quotation omitted); *FW/PBS, Inc. v. Dallas*, 493 U.S. 215, 225-27 (1990) (plurality opinion). Defendants’ prior restraint inflicts both evils.

a. Unbridled Discretion to Censor Speech.

“Statutes or policies” affording government officials “unbridled discretion” to determine “who may speak and who may not . . . are unconstitutional.” *City of Lakewood v. Plain Dealer Publ’g Co.*, 486 U.S. 750, 763 (1988) (citations omitted). “[E]ven if the government may constitutionally impose content-neutral prohibitions on a particular manner of speech, it may not *condition* that speech on obtaining a license or permit from a government official in that official’s boundless discretion.” *Id.* at 763-64. Accordingly, standards governing prior restraints must be “narrow, objective and definite.” *Shuttlesworth v. Birmingham*, 394 U.S. 147, 151 (1969). Standards involving “appraisal of facts, the exercise of judgment, [or] the formation of an opinion” are unacceptable. *Forsyth County v. Nationalist Movement*, 505 U.S. 123, 131 (1992) (quotation omitted). “Unbridled discretion naturally exists when a licensing scheme does not impose adequate standards to guide the licensor’s discretion.” *Chesapeake B & M, Inc. v. Harford County*, 58 F.3d 1005, 1009 (4th Cir. 1995) (en banc).

ITAR does not meaningfully limit Defendants’ discretion. Reasonable persons must guess at what “specially designed” or “military application” truly mean and there are no limits to what DDTC can claim falls under USML Category XXI. Were Defendants able to readily apply their criteria, perhaps Defense Distributed’s ten pending commodity jurisdiction requests would not

remain outstanding for nearly two years. “‘Technical data’ is perhaps the most confusing category of items regulated by the ITAR since it is defined separately and in relation to defense articles, 22 C.F.R. § 120.10, but is also defined as a defense article when it is covered by the USML. *See* 22 C.F.R. § 120.6.” *Bernstein I*, 945 F. Supp. at 1284. Indeed, the regulations explicitly bar publication of a “Not Otherwise Enumerated” class of “technical data.” 22 C.F.R. § 121.1 at USML paragraph XXI(b). An unenumerated prior restraint is the very definition of unbridled discretion. Respectfully, “if doubt exists as to whether [speech] is covered by the U.S. Munitions List,” the solution should not be found in Defendants’ inscrutable and often interminable “commodity jurisdiction” procedures. 22 C.F.R. § 120.4(a). Rather, the solution should be found in a judicial declaration that ITAR’s speech controls must conform to First Amendment requirements.

b. Lengthy Delays and the Lack of Procedural Safeguards.

“[T]he Supreme Court established three procedural safeguards to protect against the suppression of constitutionally protected speech by a censorship board.” *Fantasy Ranch, Inc. v. City of Arlington*, 459 F.3d 546, 563 (5th Cir. 2006) (citing *Freedman*).

First, any restraint before judicial review occurs can be imposed only for a specified brief period during which the status quo must be maintained; second, prompt judicial review of that decision must be available; and third, the censor must bear the burden of going to court to suppress the speech and must bear the burden of proof in court.

Id. (quotation omitted).

“The ITAR scheme, a paradigm of standardless discretion, fails on every count.” *Bernstein I*, 945 F. Supp. at 1289. The DOPSR review process contains no publicly-known timelines in which the agency must complete its review. Aggravating this situation, in cases where DOPSR refuses to perform its review because of uncertain export control jurisdiction, as noted above, the period of time it takes to obtain a commodity jurisdiction request to enable DOPSR review can take months to

a year or more. Defense Distributed's ten commodity jurisdiction requests regarding the previously Published Files have been pending at DDTC for nearly two years—a long time throughout which Defense Distributed has been threatened with criminal enforcement should it republish the files.

And in cases where DOPSR refuses to allow publication and requires that a license be obtained from Defendants, nothing requires DDTC to issue a licensing decision within a specific and reasonable period of time. Relevant here, a “Policy on Review Time for License Applications” established under a 2008 National Security Decision Directive requires that DDTC “complete the review and adjudication of license applications within 60 days of receipt.” *See* 74 Fed. Reg. 63497 (December 3, 2009). A two-month delay on the right to speak is per se unreasonable under the First Amendment. But even were a two-month delay constitutional, this policy contains broad “national security exceptions” allowing the government plenary authority to override the timeline. This exception effectively swallows the two month rule, as it applies where “[t]he Department of Defense has not yet completed its review” and “[w]hen a related export policy is under active review and pending final determination by the Department of State.” *Id.* A prior restraint that “permits a delay without limits” is unconstitutional. *Riley v. Nat’l Fed. of Blind of N.C.*, 487 U.S. 781, 802 (1988).

And although “only a judicial determination in an adversary proceeding ensures the necessary sensitivity to freedom of expression, only a procedure requiring a judicial determination suffices to impose a valid final restraint,” *Freedman*, 380 U.S. at 59, judicial review of DDTC or DOPSR actions is non-existent. In fact, ITAR expressly provides that Defendants’ licensing determinations are *not* subject to judicial review under the Administrative Procedures Act. 22 C.F.R. § 128.1. And the AECA provides that “[t]he designation . . . of items as defense articles or defense services for purposes of this section shall not be subject to judicial review.” 22 U.S.C. § 2778(h).

4. Defendants’ Speech Regulation of Plaintiffs’ Speech Fails Any Level of First Amendment Scrutiny.

“Premised on mistrust of governmental power, the First Amendment stands against attempts to disfavor certain subjects or viewpoints.” *Citizens United v. FEC*, 558 U.S. 310, 340 (2010) (citations omitted). “[A]s a general matter, the First Amendment means that government has no power to restrict expression because of its message, its ideas, its subject matter, or its content.” *Stevens*, 559 U.S. at 468 (quotation omitted). A speech restriction is “content based if it require[s] enforcement authorities to examine the content of the message that is conveyed to determine whether a violation has occurred.” *McCullen v. Coakley*, 134 S. Ct. 2518, 2531 (2014) (quotation omitted). This aptly describes Defendants’ prior restraint. Plaintiffs are free to publish whatever they want, on the Internet or anywhere else, unless Defendants deem the content of Plaintiffs’ speech to be ITAR-controlled.

It does not matter that Defendants might claim to be indifferent to any views expressed in Plaintiffs’ speech. The absence of “illicit legislative intent” or an “improper censorial motive” is irrelevant when considering that Defendants’ restriction is content-based. *Simon & Schuster, Inc. v. Members of the N.Y. State Crime Victims Bd.*, 502 U.S. 105, 117 (1991) (quotations omitted). Defendants have singled out speech about arms—and “the First Amendment’s hostility to content-based regulation extends not only to a restriction on a particular viewpoint, but also to a prohibition of public discussion of an entire topic.” *Burson v. Freeman*, 504 U.S. 191, 197 (1992) (plurality opinion) (citations omitted).

“Since [Defendants’ practice] is a content-based speech restriction, it can stand only if it satisfies strict scrutiny.” *United States v. Playboy Entm’t Group*, 529 U.S. 803, 813 (2000) (citation omitted). This much, it cannot do. While Defendants may have a compelling interest in

controlling the export of sensitive data related to certain defense articles, the restriction is not narrowly tailored, reaching vastly more speech than needed to advance the regulatory interest, and capturing vastly more speech than that intended for a foreign audience.

C. DEFENDANTS' PRIOR RESTRAINT IS VOID FOR VAGUENESS.

"It is a basic principle of due process that an enactment is void for vagueness if its prohibitions are not clearly defined." *Grayned v. City of Rockford*, 408 U.S. 104, 108 (1972). Vagueness doctrine applies with particular force in review of laws dealing with speech. "[S]tricter standards of permissible statutory vagueness may be applied to a statute having a potentially inhibiting effect on speech; a man may the less be required to act at his peril here, because the free dissemination of ideas may be the loser." *Hynes v. Mayor & Council of Oradell*, 425 U.S. 610, 620 (1976) (quotations omitted). "Under the First and Fifth Amendments, speakers are protected from arbitrary and discriminatory enforcement of vague standards.'" *Nat'l Endowment for the Arts v. Finley*, 524 U.S. 569, 588 (1998) (citation omitted).

Defendants' prepublication approval requirement is by no means self-evident to reasonable people reading the ITAR. If anything, ITAR's exclusion of information in the public domain suggests a variety of avenues by which people might avoid ITAR's strictures by publishing their information. The regulatory regime has even been amended to remove the suggestion of a pre-publication review requirement, the validity of which the Justice Department has repeatedly questioned. The existence of a catch-all provision, and the need to submit to the opaque commodity jurisdiction procedures, confirm that persons of "common intelligence must necessarily guess at [ITAR's] meaning and differ as to its application." *Connally v. General Const. Co.*, 269 U.S. 385, 391 (1926) (citations omitted). It thus "violates the first essential of due process of law." *Id.*

D. DEFENDANTS ARE VIOLATING PLAINTIFFS’ SECOND AMENDMENT RIGHTS.

1. *The Government Bears the Burden of Proving that Laws Burdening Second Amendment Rights Pass Heightened Scrutiny Review.*

The Second Amendment functions as a normal constitutional right. As the Supreme Court demonstrated, some laws will be struck down for conflicting with the right’s core guarantee, without employing any balancing test. *District of Columbia v. Heller*, 554 U.S. 570 (2008). In *Heller*, once it was determined that the Second Amendment secures a right to have handguns for self-defense, city ordinances banning handguns and the keeping of functional firearms simply could not survive. “The Court invalidated the laws because they violated the central right that the Second Amendment was intended to protect” *Nat’l Rifle Ass’n of Am., Inc. v. Bureau of Alcohol, Tobacco, Firearms & Explosives*, 700 F.3d 185, 193 (5th Cir. 2012) (“*NRA*”). Other cases lend themselves to different constitutional tests, *e.g.*, gun licensing laws affording unbridled discretion could be viewed as prior restraints, and disarmed individuals may raise as-applied challenges based on their personal circumstances.

But in large part, when Second Amendment claims arise,

[a] two-step inquiry has emerged as the prevailing approach: the first step is to determine whether the challenged law impinges upon a right protected by the Second Amendment—that is, whether the law regulates conduct that falls within the scope of the Second Amendment’s guarantee; the second step is to determine whether to apply intermediate or strict scrutiny to the law, and then to determine whether the law survives the proper level of scrutiny.

NRA, 700 F.3d at 194 (citations omitted). The Fifth Circuit follows this approach in appropriate cases, *Id.*, and this case appears to be well-suited to this approach.

“To determine whether a law impinges on the Second Amendment right, we look to whether the law harmonizes with the historical traditions associated with the Second Amendment guarantee.” *Id.* (citations omitted). “If the challenged law burdens conduct that falls outside the Second

Amendment's scope, then the law passes constitutional muster. If the law burdens conduct that falls within the Second Amendment's scope, we then proceed to apply the appropriate level of means-ends scrutiny." *Id.* at 195 (citations omitted).

"[T]he appropriate level of scrutiny depends on the nature of the conduct being regulated and the degree to which the challenged law burdens the right." *NRA*, 700 F.3d at 195 (citations omitted). But at least in the Fifth Circuit, rational basis review is unavailable. Means-ends scrutiny in Second Amendment cases must always be heightened scrutiny—strict or intermediate. *Id.*

2. *The Second Amendment Secures the Right to Produce Firearms, and to Exchange Technical Data Concerning Firearms.*

There is no question that the Second Amendment secures a right to possess firearms, including handguns such as the Liberator. *See Heller*. Because individuals have the right to render their firearms operable as such (and not be mere paperweights), *Heller*, 554 U.S. at 630, it follows that constitutional protection extends to any components necessary to the functioning of one's constitutionally-protected firearm.

But there must be more. "[C]ertain unarticulated rights are implicit in enumerated guarantees . . . fundamental rights, even though not expressly guaranteed, have been recognized by the Court as indispensable to the enjoyment of rights explicitly defined." *Richmond Newspapers v. Virginia*, 448 U.S. 555, 579-80 (1980). Because there is a right to possess handguns, there is, necessarily, a right to acquire them. And the most basic means of acquiring something, is to make it. Surely, the Second Amendment secures the right to make the arms that might then be kept or carried. *Cf. Martin v. Harrington & Richardson, Inc.*, 743 F.2d 1200, 1204 (7th Cir. 1984) (adopting tort doctrines "which would in practice drive [handgun] manufacturers out of business, would produce a handgun ban by judicial fiat in the face of" a constitutional right to handgun

possession.”). If “restricting the ability to purchase an item is tantamount to restricting that item’s use,” *Reliable Consultants, Inc. v. Earle*, 517 F.3d 738, 743 (5th Cir. 2008) (footnote omitted), the same must be said of restricting the ability to manufacture that item.¹⁰

The fact manufactured arms might cross the Nation’s borders does not diminish the right to arms. “Our citizens have always been free to make, vend and export arms. It is the constant occupation and livelihood of some of them.” 3 THE WRITINGS OF THOMAS JEFFERSON 230 (T.J. Randolph, ed., 1830). “With organized armories inaccessible to the frontier and low barriers to entering the trade in all regions, the [early American] public could reasonably have understood a right to acquire arms through self-production.” Peter Jensen-Haxel, *3D Printers, Obsolete Firearm Supply Controls, and the Right to Build Self-Defense Weapons Under Heller*, 42 Golden Gate U. L. Rev. 447, 478 (2012).

In keeping with the familiar rule “vendors and those in like positions . . . have been uniformly permitted to resist efforts at restricting their operations by acting as advocates for the rights of third parties who seek access to their market or function,” *Carey v. Pop. Servs. Int’l*, 431 U.S. 678, 684 (1977) (quotation omitted); *Reliable Consultants*, 517 F.3d at 743, Plaintiffs are entitled to assert the Second Amendment rights of their customers and website visitors. “[O]perating a business that provides Second Amendment services is generally protected by the Second Amendment.” *Mance v. Holder*, No. 4:14-cv-539-O, 2015 U.S. Dist. LEXIS 16679, at *25 n.8 (N.D. Tex. Feb. 11, 2015); *Ezell v. City of Chicago*, 651 F.3d 684, 696 (7th Cir. 2011) (“Action

¹⁰In *United States v. Henry*, 688 F.3d 637 (9th Cir. 2012), the Ninth Circuit rejected a Second Amendment claim to a homemade machine gun. Notably, the court did not address, let alone deny that the Second Amendment secures the right to make firearms. Rather, the court held that this particular type of firearm lies outside the Second Amendment’s scope. Plaintiffs do not claim a right in any arms or arms components that would lack Second Amendment protection.

Target, as a supplier of firing-range facilities, is harmed by the firing-range ban”). And SAF has associational standing to assert its members Second Amendment rights. *Mance*, at *11-*12.

3. *Defendants’ Regulations Fail Any Level of Second Amendment Scrutiny.*

The prior restraint and prohibition of speech relating to the manufacture of firearms and related components is very much “a salient outlier in the historical landscape of gun control.” *NRA*, 700 F.3d at 205. Never mind the Framing Era—nothing like this has existed in the United States until Defendants ordered the Liberator files taken down. As the record shows, ITAR was long ago amended specifically to remove the suggestion of such prior restraints. And while the Government’s various opinions over the years have focused on the scheme’s First Amendment problems, the fact remains that this type of conduct lies well outside American tradition and accepted legal norms.

“A regulation that threatens a right at the core of the Second Amendment—for example, the right of a law-abiding, responsible adult to possess and use a handgun to defend his or her home and family—triggers strict scrutiny.” *NRA*, 700 F.3d at 195; *see also United States v. Masciandaro*, 638 F.3d 458, 470 (4th Cir. 2011) (“we assume that any law that would burden the ‘fundamental,’ core right of self-defense in the home by a law-abiding citizen would be subject to strict scrutiny”). Defendants’ restrictions squarely fit this description, though the outcome would be no different under intermediate scrutiny, which “requires the government to demonstrate a ‘reasonable fit’ between the challenged regulation and an ‘important’ government objective,” *NRA*, 700 F.3d at 195, and “may not burden more [conduct] than is reasonably necessary,” *United States v. Marzzarella*, 614 F.3d 85, 98 (3d Cir. 2010).

Again, Plaintiffs do not question that the Government has a compelling interest in regulating the exportation of arms. But this interest cannot effectively override the traditional, centuries-old American craft of making arms of the kind to which individuals in this country enjoy a fundamental

right. If allowing Americans to exchange information useful in the manufacture of Second Amendment arms carries some risk that the information might be gleaned by a foreign government, there are nonetheless real limits on the Government’s ability to mitigate that (theoretical) harm. The later-enacted Second Amendment acts as a limitation on Congress’s authority to regulate foreign commerce, and not the other way around.

* * *

Plaintiffs are substantially likely to prevail on at least some if not all of their claims.

II. DEFENDANTS’ LICENSING SCHEME IRREPARABLY HARMS PLAINTIFFS.

A finding that a constitutional right “‘is either threatened or in fact being impaired’ . . . mandates a finding of irreparable injury.” *Deerfield Med. Center v. City of Deerfield Beach*, 661 F.2d 328, 338 (5th Cir. 1981) (quoting *Elrod v. Burns*, 427 U.S. 347, 373 (1976)). “The loss of First Amendment freedoms, for even minimal periods of time, unquestionably constitutes irreparable injury.” *Elrod*, 427 U.S. at 373-74 (citations omitted). And no constitutional right is so directly linked to one’s immediate physical well-being as is the right to keep and bear arms. The interest in self-defense is the “*central component* of the [Second Amendment] right itself,” *Heller*, 554 U.S. at 599 (emphasis original). As the Seventh Circuit explained,

The loss of a First Amendment right is frequently presumed to cause irreparable harm based on “the intangible nature of the benefits flowing from the exercise of those rights; and the fear that, if those rights are not jealously safeguarded, persons will be deterred, even if imperceptibly, from exercising those rights in the future.” The Second Amendment protects similarly intangible and unquantifiable interests. *Heller* held that the Amendment’s central component is the right to possess firearms for protection. Infringements of this right cannot be compensated by damages.

Ezell, 651 F.3d at 699 (citations and footnote omitted).

III. THE BALANCE OF EQUITIES FAVORS GRANTING INJUNCTIVE RELIEF.

While Plaintiffs suffer irreparable harm when their fundamental rights are violated, an injunction would not harm Defendants at all. First, it appears that Defendants have thus far targeted only Defense Distributed’s website with a prior restraint on unclassified technical data. Defendants are not apparently taking action to control all technical data, or even just unclassified technical data relating to arms, present throughout the public domain. And an injunction would not bar Defendants from controlling the export of classified information.

IV. THE PUBLIC INTEREST WARRANTS INJUNCTIVE RELIEF.

“[I]t is always in the public interest to prevent the violation of a party’s constitutional rights.” *Jackson Women’s Health Org. v. Currier*, 760 F.3d 448, 458 n.9 (5th Cir. 2014) (quoting *Awad v. Ziriax*, 670 F.3d 1111, 1132 (10th Cir. 2012)); *De Leon v. Perry*, 975 F. Supp. 2d 632, 665 (W.D. Tex. 2014).

V. NO BOND OR OTHER SECURITY IS REQUIRED AS A CONDITION OF INJUNCTIVE RELIEF.

The security requirement of Fed. R. Civ. P. 65(c) may be dispensed with when there is no risk of financial harm to the enjoined party. “In holding that the amount of security required pursuant to Rule 65(c) ‘is a matter for the discretion of the trial court,’ we have ruled that the court ‘may elect to require no security at all.’” *Kaepa, Inc. v. Achilles Corp.*, 76 F.3d 624, 628 (5th Cir. 1996) (quotation and citations omitted). Even courts that view Rule 65(c) as mandatory are open to the idea of the mandatory bond being set at zero. *See Hoechst Diafoil Co. v. Nan Ya Plastics Corp.*, 174 F.3d 411, 421 n.3 (4th Cir. 1999). As an injunction would not financially harm Defendants, the Court should dispense with the bond requirement.

CONCLUSION

Plaintiffs respectfully request that the motion be granted.

Dated: May 11, 2015

Respectfully submitted,

GURA & POSSESSKY, PLLC

FISH & RICHARDSON P.C.

Alan Gura
Virginia Bar No. 68842*
Gura & Possessky, PLLC
105 Oronoco Street, Suite 305
Alexandria, Virginia 22314
703.835.9085 / Fax 703.997.7665
alan@gurapossessky.com

/s/ William B. Mateja
William T. "Tommy" Jacks
Texas State Bar No. 10452000
William B. Mateja
Texas State Bar No. 13185350
David S. Morris
Texas State Bar No. 24032877
FISH & RICHARDSON P.C.
One Congress Plaza, Suite 810
111 Congress Avenue
Austin, Texas 78701
(512) 472-5070 (Telephone)
(512) 320-8935 (Facsimile)
jacks@fr.com
dmorris@fr.com
mateja@fr.com

Matthew Goldstein
D.C. Bar No. 975000*
Matthew A. Goldstein, PLLC
1012 14th Street NW, Suite 620
Washington, DC 20005
202.550.0040/Fax 202.683.6679
matthew@goldsteinpllc.com

Josh Blackman
Virginia Bar No. 78292*
1303 San Jacinto Street
Houston, Texas 77002
202.294.9003/Fax: 713.646.1766
joshblackman@gmail.com

*Admission pro hac vice pending

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
AUSTIN DIVISION

DEFENSE DISTRIBUTED and	§	Case No. 15-CV-372-RP
SECOND AMENDMENT FOUNDATION, INC.,	§	
	§	
Plaintiffs,	§	
	§	
v.	§	
	§	
U.S. DEPARTMENT OF STATE, et al.,	§	
	§	
Defendants.	§	
-----	§	

APPENDIX IN SUPPORT OF
PLAINTIFFS' MOTION FOR PRELIMINARY INJUNCTION

Contents

Declaration of Cody Wilson.	App. 1
Declaration of Alan Gottlieb.	App. 6
Declaration of Conn Williamson	App. 8
Declaration of Peter Versnel.	App. 10
Exhibit 1 - DDTC Enforcement Division Letter (May 8, 2013)	App. 12
Exhibit 2 - Washington Trade & Tariff Letter, Vo. 29, No. 31.	App. 16
Exhibit 3 - GAO Publication No. GAO-02-996.....	App. 21
Exhibit 4 - Office of Inspector General Memorandum Report 01-FP-M-027.	App. 76
Exhibit 5 - DDTC June 3, 2014 Website Notice.	App. 91
Exhibit 6 - 1978 Department of Justice Opinion.	App. 98
Exhibit 7 - 1981 Department of Justice Opinion (ITAR).....	App. 116

Exhibit 8 - 1981 Department of Justice Opinion (EAR).	App. 130
Exhibit 9 - 1984 Department of Justice Opinion.	App. 136
Exhibit 10 - 1997 Department of Justice Report.	App. 152
Exhibit 11 - 22 C.F.R. § 125.11 (1978).	App. 197
Exhibit 12 - Munitions Control Newsletter No. 80.. . . .	App. 204
Exhibit 13 - Defense Distributed Ten Commodity Jurisdiction Requests (June 21, 2013)..	App. 207
Exhibit 14 - Defense Distributed DOPSR Request (September 25, 2014).	App. 260
Exhibit 15 - DOPSR Refusal to Review Request (October 1, 2014).	App. 263
Exhibit 16 - Ghost Gunner Commodity Jurisdiction Request (January 2, 2015).	App. 266
Exhibit 17 - DDTC Final Determination on Ghost Gunner (April 15, 2015).	App. 279
Exhibit 18 - Defense Distributed DOPSR Request (September 2, 2014).	App. 282
Exhibit 19 - Defense Distributed DOPSR Request (October 9, 2014-C).	App. 286
Exhibit 20 - Defense Distributed DOPSR Request (October 9, 2014-M).	App. 290
Exhibit 21 - Defense Distributed DOPSR Request (October 23, 2014).	App. 294
Exhibit 22 - DOPSR Refusal to Review Request (December 31, 2014).	App. 298
Exhibit 23 - Defense Distributed Request for Advisory Opinion (January 5, 2015).	App. 305

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
AUSTIN DIVISION

DEFENSE DISTRIBUTED and
SECOND AMENDMENT FOUNDATION, INC.,

Plaintiffs,

V.

U.S. DEPARTMENT OF STATE, et al.,

Defendants.

Case No. 15-CV-372

DECLARATION OF CODY WILSON

I, Cody Wilson, declare:

1. I am a citizen of the United States and a resident of Texas.
2. I co-founded and now lead Defense Distributed, a Texas non-profit corporation.

Defense Distributed is organized and operated for the purpose of defending the civil liberty of popular access to arms guaranteed by the United States Constitution through facilitating global access to, and the collaborative production of, information and knowledge related to the 3D printing of arms; and to publish and distribute, at no cost to the public, such information and knowledge on the Internet in promotion of the public interest.

3. Beginning in 2012, Defense Distributed privately generated, and posted on the Internet for free access by the public, technical information about various gun-related items, including a trigger guard, grips, two receivers, a magazine for AR-15 rifles, and a handgun named “The Liberator” (the “Published Files”). At the time it did so, there were no publicly known DDTC enforcement actions for the posting of files on the Internet.

4. The Published Files were downloaded hundreds of thousands times. The Liberator files in particular generated national media attention, with coverage in Forbes, CNN, NBC News, the Wall Street Journal, and even an episode of The Colbert Report.

5. In May 2013, Defense Distributed received a letter dated May 8, 2013, from Glenn Smith, Chief of Defendant DDTC's Enforcement Division. The letter warned:

DTCC/END is conducting a review of technical data made publicly available by Defense Distributed through its 3D printing website, DEFCAD.org, the majority of which appear to be related to items in Category I of the USML. Defense Distributed may have released ITAR-controlled technical data without the required prior authorization from the Directorate of Defense Trade Controls (DDTC), a violation of the ITAR . . . all such data should be removed from public access immediately.

Exhibit 1 is a true and correct copy of that letter.

6. At the time it posted the Published Files, Defense Distributed did not know that the government would demand to pre-approve its speech. Defense Distributed believed, and continues to believe, that the United States Constitution guarantees a right to share truthful speech—especially speech concerning fundamental constitutional rights—in open forums. Nevertheless, for fear of criminal and civil enforcement, Defense Distributed promptly complied with Defendants' demands and removed all of the Published Files from its servers.

7. Defendants' letter further directed Defense Distributed to submit the Published Files to DDTC for review using the "commodity jurisdiction" procedure. Defense Distributed complied with Defendants' request and filed ten (10) commodity jurisdiction requests covering the Published Files on June 21, 2013. Exhibit 13 is a true and correct copy of those requests (without attachments). Nearly two years later, Defendants have still not responded to the requests.

8. On September 25, 2014, Defense Distributed requested DOPSR's prepublication approval for public release of files containing technical information on a milling machine, named the "Ghost Gunner," that can be used to manufacture a variety of items, including gun parts (the "Ghost Gunner Files").¹ Exhibit 14 is a true and correct copy of that request (without attachments). On October 1, 2014, DOPSR informed Defense Distributed this request for review was refused because DOPSR was unsure whether the Ghost Gunner was subject to ITAR. DOPSR further recommended that Defense Distributed submit another commodity jurisdiction request to the Defendants. Exhibit 15 is a true and correct copy of DOPSR's October 1, 2014 correspondence to Defense Distributed.

9. Defense Distributed submitted another commodity jurisdiction request for the Ghost Gunner to Defendants on January 2, 2015. Exhibit 16 is a true and correct copy of that request (without attachments). On April 15, 2015, Defendant DDTC determined that the Ghost Gunner machine, user manual, and operating software are not subject to ITAR, but that "software, data files, project files, coding, and models for producing a defense article, to include 80% AR-15 lower receivers, are subject to the jurisdiction of the Department of State in accordance with [ITAR]." Exhibit 17 is a true and correct copy of DOPSR's April 15, 2015 correspondence to Defense Distributed.

10. Since September 2, 2014, Defense Distributed has made multiple requests to DOPSR for prepublication review of certain computer-aided design ("CAD") files. Exhibits 18 through 21 are true and correct copies of these requests (without attachments). On December 31,

¹Any milling machine can be modified to mill components that are unlawful to manufacture, just as any saw that may be purchased at a hardware store can be used to unlawfully shorten a shotgun. However, Ghost Gunner does not ship with the jigs and code to

2014, nearly four months after the first such review request, DOPSR sent Defense Distributed two letters dated December 22, 2014, stating its refusal to review the CAD files. The letters directed Defense Distributed to the DDTC Compliance and Enforcement Division for further questions on public release of the CAD files. Exhibit 22 is a true and correct copy of DOPSR's December 31, 2014 correspondence to Defense Distributed.

11. However, because this is not the DDTC division responsible for issuing licenses or other DDTC authorizations, on January 5, 2015, Defense Distributed requested Defendants' guidance on how to obtain authorization from DDTC Compliance for release of the CAD files. Exhibit 23 is a true and correct copy of that request (without attachments). To date, Defendants have not responded to Defense Distributed's request for guidance.

12. Defense Distributed appears to be the ITAR prior restraint scheme's *only* target. Other websites containing similar firearm-related parts, such as GrabCAD.com, Weaponeer.com, Thingiverse.com, Ak-builder.com, AR15.com, Scribd.com, CNCguns.com, we are apparently unimpeded.

13. Defense Distributed has and will continue to create and possess other files that contain technical information, to include design drawings, rendered images, written manufacturing instructions, and other technical information that Defense Distributed intends to post to open forums on the Internet. Many of these files are described in the USML.

14. But for Defendants' impositions upon the distribution of the Published Files, Ghost Gunner Files, CAD Files, and Defense Distributed's other files (collectively, the "Subject Files"), Defense Distributed would freely distribute the Subject Files and other files relating to

manufacture machine guns, and Defense Distributed has no intention of offering such items for sale.

Second Amendment arms. Defense Distributed refrains from distributing the Subject Files because I fear that Defendants would pursue criminal and civil enforcement proceedings against me and the company for doing so.

I declare under penalty of perjury that the foregoing is true and correct.

This the 8th day of May, 2015.


Cody Wilson

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
AUSTIN DIVISION

DEFENSE DISTRIBUTED and	§	Case No. 15-CV-372-RP
SECOND AMENDMENT FOUNDATION, INC.,	§	
	§	
Plaintiffs,	§	
	§	
v.	§	
	§	
U.S. DEPARTMENT OF STATE, et al.,	§	
	§	
Defendants.	§	
	§	

DECLARATION OF ALAN GOTTLIEB

I, Alan Gottlieb, declare:

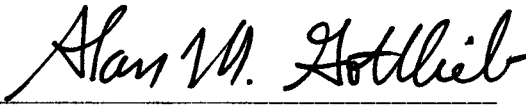
1. I am a citizen of the United States and a resident of the state of Washington.
2. I am the Executive Vice President of the Second Amendment Foundation, Inc. (SAF). SAF is a non-profit membership organization incorporated under the laws of Washington with its principal place of business in Bellevue, Washington. SAF has over 650,000 members and supporters nationwide, including Texas. The purposes of SAF include education, research, publishing and legal action focusing on the constitutional right to privately own and possess firearms, and the consequences of gun control.
3. The issues raised by, and consequences of, Defendants' policies, are of great interest to SAF's constituency. Conn Williamson and Peter Versnel are members of SAF. Countless other law-abiding, responsible adult SAF members and supporters would access, study, share, modify, and learn from Defense Distributed's various files, as well as similar 3D printing files related to firearms that they or others have created. SAF members would create and share firearm 3-D printing files.

4. In furtherance of SAF's mission, and to serve its members and the public, SAF would publish and promote, on the Internet, the free distribution of Defense Distributed's various files, and allow its members and others to upload their own 3-D printing firearm-related files to SAF's servers for Internet publication. SAF is presently refraining from doing so only owing to the Government's interpretation of ITAR, including threats against Defense Distributed.

5. SAF is proud to bring this action on behalf of its members.

I declare under penalty of perjury that the foregoing is true and correct.

Executed this the 7th day of May, 2015.



Alan Gottlieb

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
AUSTIN DIVISION

DEFENSE DISTRIBUTED and
SECOND AMENDMENT FOUNDATION, INC.,

Plaintiffs,

v.

U.S. DEPARTMENT OF STATE, et al.,

Defendants.

§ Case No. _____
§
§
§
§
§
§
§
§
§
§

DECLARATION OF CONN WILLIAMSON

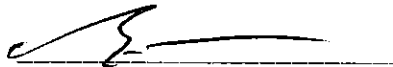
I, Conn Williamson, declare:

1. I am a citizen of the United States and a resident of the state of Washington.
2. I am over the age of 21, am not under indictment, have never been convicted of a felony or misdemeanor crime of domestic violence, am not a fugitive from justice, am not an unlawful user of or addicted to any controlled substance, have never been adjudicated a mental defective or committed to a mental institution, have never been discharged from the Armed Forces under dishonorable conditions, have never renounced my citizenship, and have never been the subject of a restraining order relating to an intimate partner.
3. I am a member of the Second Amendment Foundation.
4. I have a keen interest in accessing, studying, sharing, modifying, and learning from Defense Distributed's various files, including files related to the Liberator handgun, as well as similar 3D printing files related to firearms that Defense Distributed or others have created. I am also interested in creating and sharing with others my own firearm 3-D printing files.

5. I have sought to download firearm files from Defense Distributed, but could not locate them on Defense Distributed's website. I understand those files were taken down owing to threats issued by government officials. Such threats also dissuade me from publishing any 3-D firearm printing files that I might create. But for the government's threats of arrest and prosecution, I would access and share 3-D printing files related to firearms.

I declare under penalty of perjury that the foregoing is true and correct.

This the 6 day of May, 2015.



Conn Williamson

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
AUSTIN DIVISION

DEFENSE DISTRIBUTED and
SECOND AMENDMENT FOUNDATION, INC.,

Plaintiffs,

v.

U.S. DEPARTMENT OF STATE, et al.,

Defendants.

§ Case No. _____
§
§
§
§
§
§
§
§
§
§

DECLARATION OF PETER VERSNEL

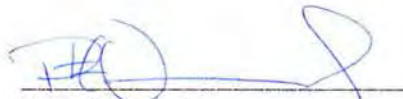
I, Peter Versnel, declare:

1. I am a citizen of the United States and a resident of the state of Washington.
2. I am over the age of 21, am not under indictment, have never been convicted of a felony or misdemeanor crime of domestic violence, am not a fugitive from justice, am not an unlawful user of or addicted to any controlled substance, have never been adjudicated a mental defective or committed to a mental institution, have never been discharged from the Armed Forces under dishonorable conditions, have never renounced my citizenship, and have never been the subject of a restraining order relating to an intimate partner.
3. I am a member of the Second Amendment Foundation.
4. I have a keen interest in accessing, studying, sharing, modifying, and learning from Defense Distributed's various files, including files related to the Liberator handgun, as well as similar 3D printing files related to firearms that Defense Distributed or others have created. I am also interested in creating and sharing with others my own firearm 3-D printing files.

5. I have sought to download firearm files from Defense Distributed, but could not locate them on Defense Distributed's website. I understand those files were taken down owing to threats issued by government officials. Such threats also dissuade me from publishing any 3-D firearm printing files that I might create. But for the government's threats of arrest and prosecution, I would access and share 3-D printing files related to firearms.

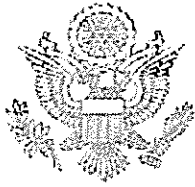
I declare under penalty of perjury that the foregoing is true and correct.

This the 6 day of May, 2015.



Peter Versnel

EXHIBIT 1



United States Department of State

*Bureau of Political-Military Affairs
Office of Defense Trade Controls Compliance
Washington, D.C. 20522-0112*

MAY 08 2013

In reply refer to

████████████████████
Mr. Cody Wilson
Defense Distributed
████████████████████
████████████████████
████████████████████

Dear Mr. Wilson:

The Department of State, Bureau of Political Military Affairs, Office of Defense Trade Controls Compliance, Enforcement Division (DTCC/END) is responsible for compliance with and civil enforcement of the Arms Export Control Act (22 U.S.C. 2778) (AECA) and the AECA's implementing regulations, the International Traffic in Arms Regulations (22 C.F.R. Parts 120-130) (ITAR). The AECA and the ITAR impose certain requirements and restrictions on the transfer of, and access to, controlled defense articles and related technical data designated by the United States Munitions List (USML) (22 C.F.R. Part 121).

DTCC/END is conducting a review of technical data made publicly available by Defense Distributed through its 3D printing website, DEF CAD.org, the majority of which appear to be related to items in Category I of the USML. Defense Distributed may have released ITAR-controlled technical data without the required prior authorization from the Directorate of Defense Trade Controls (DDTC), a violation of the ITAR.

Technical data regulated under the ITAR refers to information required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance or modification of defense articles, including information in the form of blueprints, drawings, photographs, plans, instructions or documentation. For a complete definition of technical data, see § 120.10 of the ITAR. Pursuant to § 127.1 of the ITAR,

it is unlawful to export any defense article or technical data for which a license or written approval is required without first obtaining the required authorization from the DDTC. Please note that disclosing (including oral or visual disclosure) or transferring technical data to a foreign person, whether in the United States or abroad, is considered an export under § 120.17 of the ITAR.

The Department believes Defense Distributed may not have established the proper jurisdiction of the subject technical data. To resolve this matter officially, we request that Defense Distributed submit Commodity Jurisdiction (CJ) determination requests for the following selection of data files available on DEFCAD.org, and any other technical data for which Defense Distributed is unable to determine proper jurisdiction:

1. Defense Distributed Liberator pistol
2. .22 electric
3. 125mm BK-14M high-explosive anti-tank warhead
4. 5.56/.223 muzzle brake
5. Springfield XD-40 tactical slide assembly
6. Sound Moderator – slip on
7. “The Dirty Diane” 1/2-28 to 3/4-16 STP S3600 oil filter silencer adapter
8. 12 gauge to .22 CB sub-caliber insert
9. Voltlock electronic black powder system
10. VZ-58 front sight.

DTCC/END requests that Defense Distributed submit its CJ requests within three weeks of receipt of this letter and notify this office of the final CJ determinations. All CJ requests must be submitted electronically through an online application using the DS-4076 Commodity Jurisdiction Request Form. The form, guidance for submitting CJ requests, and other relevant information such as a copy of the ITAR can be found on DDTC’s website at <http://www.pmddtc.state.gov>.

Until the Department provides Defense Distributed with final CJ determinations, Defense Distributed should treat the above technical data as ITAR-controlled. This means that all such data should be removed from public access immediately. Defense Distributed should also review the remainder of the data made public on its website to

- 3 -

determine whether any additional data may be similarly controlled and proceed according to ITAR requirements.

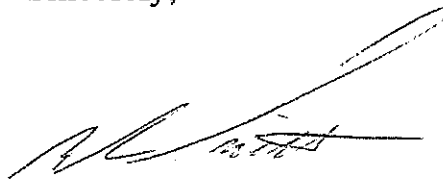
Additionally, DTCC/END requests information about the procedures Defense Distributed follows to determine the classification of its technical data, to include the aforementioned technical data files. We ask that you provide your procedures for determining proper jurisdiction of technical data within 30 days of the date of this letter to Ms. Bridget Van Buren, Compliance Specialist, Enforcement Division, at the address below:

Office of Defense Trade Controls Compliance

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

We appreciate your full cooperation in this matter. Please note our reference number in any future correspondence.

Sincerely,



Glenn E. Smith
Chief, Enforcement Division

EXHIBIT 2

ISSN 0276-8275

WTTOnline.com

A Weekly Report for Business Executives on
U.S. Trade Policies, Negotiations, Legislation,
Trade Laws and Export Controls

**Washington
Tariff & Trade
Letter®**

Editor & Publisher: Samuel M. Gilston • P.O. Box 5325, Rockville, MD 20848-5325 • Phone: 301.570.4544 Fax: 301.570.4545

Vol. 29, No. 31

August 3, 2009

NSC Issues Guidance to Speed Commodity Jurisdiction Decisions

President Obama's national security adviser, General Jim Jones, has issued new guidance aimed at shortening the deadline for State to issue Commodity Jurisdiction (CJ) decisions and creating an interagency process for resolving differences over CJ rulings. "There is now a new set of CJ procedural guidelines in place that General Jones signed about a month ago that compress the timelines" for CJ decisions, Bureau of Industry and Security (BIS) Acting Assistant Secretary Matthew Borman said July 28. "There is a regular weekly meeting between the agencies at a fairly senior level to look at CJs when there is still disagreement among the agencies," he told the BIS Sensors and Instrumentation Technical Advisory Committee (SITAC).

The new guidance was issued June 18 to State's Directorate of Defense Trade Controls (DDTC), Defense's Defense Technology Security Administration (DTSA) and BIS. It implements one of the export control reforms President Bush initiated in a National Security Policy Directive (NSPD) in January 2008. It replaces CJ guidance last updated in 1996.

The new procedures cut the deadline for completing a CJ application to 60 days from 90 days. After the application is received by DDTC and sent out to the other agencies for review and comment, BIS and DTSA must give their responses in 20 days. If there is disagreement among the agencies, a meeting of officials from the three agencies will be held within 30 days. Officials at this meeting will be at the office director or deputy assistant secretary (DAS) level. After DDTC takes this advice, it will issue a preliminary decision. If there is still disagreement, the case will be escalated to a meeting of officials at the assistant secretary level. This Interagency Policy Committee (IPC) will be chaired by an official from the White House National Security Council. The final determination will still be up to DDTC.

So far, there have been two weekly meetings of DAS-level officials. The first meeting of the IPC is scheduled for the week of Aug. 3. At the first DAS-level meeting, five pending CJs were considered and 12 were reviewed at the second. In addition to new incoming applications, the process is also working on the backlog of older pending cases. DDTC is expected to roll out the new procedures publicly, along with a new CJ application form, in August.

U.S.-China Talks Stress Close Economic Ties

That the U.S. and China are locked in an economic bear hug from which neither can let go was underscored by two days of bilateral talks July 27-28 of the newly renamed Strategic and



Economic Dialogue (S&ED) in Washington. From the opening ceremony, at which President Obama spoke, until the closing press conference, neither side wanted to upset the balance that links U.S. dependence on the Chinese buying U.S. Treasuries and China's need for the U.S. market for its exports. U.S. Trade Representative (USTR) Ron Kirk sat in on the economic talks chaired by Treasury Secretary Timothy Geithner, and several trade topics, including the pending Section 421 case on tires, were mentioned briefly along with a laundry list of issues. The main forum for trade issues, however, will be the next meeting of the Joint Commission on Commerce and Trade (JCCT) that Kirk co-chairs with Commerce Secretary Gary Locke and their Chinese counterparts. That meeting is tentatively planned for October in China.

Missing from the public statements of Secretary of State Hillary Clinton and Geithner, who co-led the U.S. side of the talks, was any public mention of last year's hot-button issue, the undervaluation of the Chinese currency. Although the topic reportedly was discussed in their closed-door meetings, the lack of public comment on the subject reflects reduced political interest in the exchange-rate issue in Congress and the greater need to assure the Chinese that their investment in U.S. bonds won't lose its value.

Instead of debating exchange rates, Chinese and American officials, including Obama, stressed the need for a more balanced economic relationship in which Americans save more and buy less and the Chinese expand domestic consumption and rely less on export-driven growth. "I think the most important thing we achieved today was to agree on this broad framework for policies and reform, both China and the United States, to help lay the foundation for a more sustainable, more balanced global recovery," Geithner told reporters July 28. "As part of that – again, this is the critical thing – that as we move to raise private savings in the United States, as we move to bring down our fiscal deficit in the future, as we move to put in place a more stable, more resilient financial system in the United States, we need to see actions in China and in other countries to shift the source of growth more to domestic demand," he said.

Chinese Vice Premier Wang Qishan said the two sides stressed the importance of taking strong measures to increase economic cooperation and trade. "The U.S. side pledged to facilitate exports of high-technology products from the United States to China," he reported. "The U.S. side is willing to step up cooperation with the Chinese side to work toward recognition of China's market economy status in an expeditious manner. The two sides will work together to support increasing investment in infrastructure, continue to advance negotiations on bilateral investment agreement, and enhance cooperation in trade finance," he added.

Obama Officials Faces Tough Choices on Model BIT

A July 29 public hearing on potential changes to the current model Bilateral Investment Treaty (BIT) the U.S. uses in investment treaties and free trade agreements sounded a lot like Goldilocks and the Three Bears. Some speakers said the current model BIT is too strong; some said it was too weak; and some said it was just right. Senior Obama administration officials will need to balance the demands from progressives for changes in the model to allow more exceptions from investment protections for environmental, natural resources and public interest concerns against business community calls for greater assurances that foreign investors will get fair and equitable treatment in BIT-signing countries. A review of the model BIT is being conducted by State and the USTR's office, with a decision on any changes expected this fall.

Sharply different views about foreign investment were seen in statements by Todd Tucker of Public Citizen's Global Trade Watch and Stephen Canner of the U.S. Council for International Business (USCIB). "The public is asking: as our domestic infrastructure is literally collapsing under our feet, why is the U.S. government promoting policies which incentivize investment abroad rather than directing it to crucial needs here at home?" Tucker testified. "BITs serve [countries] well by serving as an advertisement that the country is a good place to do business," Canner said. Critics of the BITs and foreign investment see the rules as giving undue advantages to foreign predatory investors and hurting the public interest, the environment and

domestic workers. The international business community contends the treaties protect legitimate investment from politically motivated governments and corrupt foreign courts. The structure of the model BIT is taking on more importance as the U.S. prepares to enter BIT negotiations with China, Russia India, Brazil and Vietnam.

Rep. Kevin Brady (R-Texas) was in the “don’t-touch-current-model” camp. “Now is not the time to weaken protection for U.S. companies abroad,” he told the hearing. “It would be unwise to alter the current model treaty,” he said. The 2004 model BIT “addressed most, if not all, of the criticism to be heard today,” Brady argued. Faced with potential changes to the model that might weaken investment protections, the business community might end up supporting this view.

Tucker quoted presidential candidate Barack Obama’s support for amending NAFTA and BITs to assure protection for labor and environmental rights and “to make clear that fair laws and regulations written to protect citizens in any of the three countries cannot be overridden simply at the request of foreign investors.” Among the changes Tucker advocated is new language in the model BIT to say “a Party shall not be prevented from adopting or maintaining measures relating to financial services it employs for prudential reasons, including for the protection of investors, depositors, policy holders, or persons to whom a fiduciary duty is owed by a financial services supplier, or to ensure the integrity and stability of the financial system.”

Sarah Anderson of the Institute for Policy Studies recommended amending the model to include an exception that would allow governments to impose capital controls during an economic crisis. William Warren of the Forum for Democracy and Trade, whose members include state and local governments officials, said BITs should not impede the sovereign rights of governments. In particular, the model should shun ideological proposals based on “very radical property rights” protections. USCIB’s Canner recommended strengthening BITs to assure the free transfer of capital in and out of countries. Capital controls just “cover up bad government policies,” he argued.

Business community support for strengthening BIT protections was offered by Calman Cohen, president of the Emergency Committee for American Trade, a trade group representing many multinational firms. “The Model BIT should be revised to strengthen the provisions on fair and equitable treatment, full protection and security and compensation for expropriation by requiring such treatment without linking it to customary international law,” he testified. The linkage to customary international law, which was added in 2004, provides a minimal level of protection, lower than provided under U.S. law and the BITs of most other capital exporting nations, he explained. A second change should modify the fair and equitable treatment standard to clarify that both procedural and equity protections are covered by this obligation. He proposed adopting the standard in the Administrative Procedure Act which protects against government action that is “arbitrary, capricious, [or] an abuse of discretion.”

BIS Stays Denial Order After Micei Files Appeal in Court

In two rare and perhaps unprecedented moves, Micei International of Skopje, Macedonia has filed suit in federal court to block a BIS denial order, and BIS has stayed the order pending the outcome of the case. In motions filed May 19 and May 30, Micei asked the D.C. U.S. Circuit Court to stay the denial order, set aside a default ruling issued against the firm by an administrative law judge (ALJ) and to vacate the BIS denial order based on the ALJ’s decision.

This may be the first court challenge of the BIS administrative settlement process and an ALJ’s determination under the Export Administration Regulations (EAR) since the *Iran Air* case in 1993 (see **WTTL**, July 5, 1993, page 1). The suit also is a test of BIS’ authority to use the International Emergency Economic Powers Act (IEEPA) to impose a denial of exporting privileges. The BIS stay of its order apparently moots Micei’s plea to the Circuit Court for a stay. On May 14, BIS had imposed a \$126,000 fine and a five-year denial of exporting privileges on Micei because it had dealings with Yuri Montgomery, a Macedonian who was the subject of

an earlier, separate denial order. Micei had been charged with exporting an array of products, including boots, shirts and EAR99 items. BIS based its order on an opinion by ALJ Michael Devine, who ruled that Micei had defaulted in the ALJ hearing proceedings because it had not properly responded to a proposed BIS Charging Letter and had not participated in the case.

Micei has hired attorney Clif Burns of Bryan Cave to represent it in its suit. "In its June 30 filing with the D.C. Circuit, Micei made a number of assertions and presented documentary materials that were not part of the Stay Petition it had filed with BIS," the agency's July 24 stay order notes. "BIS is continuing to evaluate and investigate questions surrounding the accuracy and foundation of those assertions, but nonetheless does not wish further delay in addressing and resolving the merits of Micei's petition for review," it adds. "In addition, Micei has recently hired new U.S.-based counsel and there are some indications that Micei may be prepared to more meaningfully engage on the issue," BIS states.

* * * **Briefs** * * *

USTR: USTR Ron Kirk tried to quash speculation that he might return to Texas to run for Senate seat being vacated by Sen. Kay Bailey Hutchinson (R-Texas), who has said she will leave Senate to run for governor of Texas. "I am happy where I am," Kirk told reporters July 31. "I am not going to resign to run for the senate now or anytime in the future. My life in politics is over," he said.

ENVIRONMENTAL EXPORTS: BIS is undertaking assessment of competitiveness of U.S. environmental products industry, including makers of solar panels, wind turbines and batteries. Study will also look at impact export controls have on these firms.

MAGNESIA CARBON BRICKS: Resco Products, Inc., July 29, filed antidumping and countervailing duty complaints at ITC and ITA against imports of magnesia carbon bricks from China and antidumping complaint against imports from Mexico.

EX-IM BANK: Bank July 16 announced new program to buy back Ex-Im guaranteed medium- and long-term export loans from banks to give banks more liquidity. "The Ex-Im Bank 'take-out' option will enable banks to offer much more competitive financing terms to their borrowers who wish to buy U.S. exports," said Ex-Im Senior Vice President John A. McAdams. If guaranteed lender exercises take-out option, Ex-Im will buy, and guaranteed lender will transfer to Bank, any loans covered by take-out option and all related transaction documents in exchange for payment of loan purchase price, Ex-Im explained. Bank will charge annual fee to lender for this option and additional fee if option is exercised.

FCPA: Helmerich & Payne entered deferred prosecution agreement with Justice July 30 and agreed to pay \$1 million penalty to settle charges that it violated FCPA with payments of bribes to government officials in Argentina and Venezuela. "The agreement recognizes H&P's voluntary disclosure and thorough self-investigation of the underlying conduct, the cooperation provided by the company to the Department, and the extensive remedial efforts undertaken by the company," Justice statement said. In separate settlement with SEC, H&P agreed to pay \$375,681 in disgorgement of profits and pre-judgment interest.

MORE FCPA: Avery Dennison of Pasadena, Calif., has entered settlements with SEC to resolve charges that it violated FCPA in connection with illegal payments its Reflectives Division of Avery (China) Co. Ltd. paid or authorized in kickbacks, sightseeing trips and gifts to Chinese government officials from 2002 to 2005. Firm agreed to cease-and-desist order barring future violations of FCPA books and records requirements. In administrative settlement, firm agreed to disgorge \$273,213 plus \$45,257 in prejudgment interest. In civil action in D.C. U.S. District Court it agreed to pay \$200,000 civil fine.

POULTRY: WTO Dispute-Settlement Body July 31 created panel to hear Chinese complaint against U.S. restrictions on imports of poultry from China. Chinese object to provision in 2009 Omnibus Appropriations Act which says "none of the funds made available in this Act may be used to establish or implement a rule allowing poultry products to be imported into the United States from the People's Republic of China." U.S. said it was disappointed by Chinese action. "As we have stated, nothing in the measure identified by China prevents the relevant U.S. authorities from continuing to work together to reach an objective, science-based response to China's request for a declaration of equivalence with respect to poultry products," U.S. statement asserted. "We also remain concerned with the way in which China has framed its panel request. In particular, we must point out again that the request appears both to include measures that were not consulted upon or do not exist and to make claims under a covered agreement pursuant to which such consultations were neither requested nor held," it added.

EXHIBIT 3

United States General Accounting Office

GAO

Report to the Chairman, Subcommittee
on National Security, Veterans Affairs,
and International Relations, Committee
on Government Reform, House of
Representatives

September 2002

EXPORT CONTROLS

Processes for Determining Proper Control of Defense-Related Items Need Improvement



G A O

Accountability * Integrity * Reliability

Contents

Letter		1
	Results in Brief	2
	Background	3
	Commerce Improperly Classified Items and Has Not Adhered to Regulatory Time Frames	5
	Commodity Jurisdiction Process Exceeded Time Frames and Is Affected by External Disagreements	12
	Conclusions	18
	Recommendations for Executive Action	19
	Agency Comments and Our Evaluation	20
	Scope and Methodology	21

Appendix I	Comments from the Department of Commerce	24
-------------------	---	-----------

Appendix II	Comments from the Department of State	39
--------------------	--	-----------

Appendix III	Comments from the Department of Defense	44
---------------------	--	-----------

Appendix IV	GAO Contact and Staff Acknowledgments	48
--------------------	--	-----------

Related GAO Products		49
-----------------------------	--	-----------

Table		
	Table 1: Commodity Classifications Completed by Commerce and Referred to State and Defense, Fiscal Years 1998-2001	6

Figures		
	Figure 1: Median Processing Times for Commodity Classifications, Fiscal Years 1998-2001	11
	Figure 2: Commodity Jurisdiction Process and Time Frames	13

Figure 3: Commodity Jurisdiction Determinations and Timeliness,
Fiscal Years 1998-2001

14



United States General Accounting Office
Washington, DC 20548

September 20, 2002

The Honorable Christopher Shays
Chairman, Subcommittee on National Security,
Veterans Affairs, and International Relations
Committee on Government Reform
House of Representatives

Dear Mr. Chairman:

The U.S. government controls the export of defense-related items to minimize the risk such exports may pose to its interests. The U.S. export control system is primarily divided between two regulatory regimes, one managed by the Department of State (State) for defense items¹ and another managed by the Department of Commerce (Commerce) for dual-use items that have both military and commercial applications. Generally, State's controls over defense items are more restrictive than Commerce's controls over dual-use items. Companies are responsible for determining which department to use and what requirements apply when exporting their items, but when in doubt can obtain government assistance through two different processes. If companies have determined that their items are Commerce-controlled but are uncertain of export licensing requirements, they may request a classification from Commerce through the commodity classification process. Commerce can refer classification requests to State and the Department of Defense (Defense) to confirm that the items are Commerce-controlled. However, if companies are unsure of which department has jurisdiction over their items, they can request a determination through the commodity jurisdiction process from State, which consults with Commerce and Defense.

Determining which department has jurisdiction over an item and how that item is controlled is fundamental to the proper implementation of the bifurcated U.S. export control system. Yet over the years, the U.S. government has experienced interagency disagreements over proper jurisdiction for items, and companies have been uncertain about which department controls the export of their items. In response to your request, we assessed how government departments assist companies in

¹ For the purposes of this report, "defense items" refers to defense articles and services as specified in the Arms Export Control Act.

determining the proper controls for defense-related items, specifically, (1) how Commerce implements the commodity classification process and (2) how State implements the commodity jurisdiction process.

Results in Brief

In implementing the commodity classification process, Commerce has improperly classified some State-controlled items as Commerce-controlled and has not adhered to regulatory time frames for responding to requests. Improper classifications have occurred because Commerce rarely obtains input from State and Defense before making decisions. Only 40 out of over 12,000 classification requests were referred by Commerce to State and Defense during the 4-year period covered by our review, even though at least 250 nonreferred requests appear to meet Commerce's referral criteria. Commerce officials told us the referral criteria are subjective and may not have been consistently applied. These officials stated they have sufficient experience to determine which items can be classified as Commerce-controlled without referring requests to State and Defense, which could delay the process. However, in several instances, Commerce improperly provided companies with classifications for State-controlled items, increasing the risk of such items being inappropriately exported. In some other instances, Commerce returned classification requests for State-controlled items to companies without notifying State, thereby limiting an opportunity for State to ensure that companies comply with statutory requirements. Commerce is also required by regulation to complete classification requests within 14 calendar days; however, Commerce took a median of 39 days to complete requests during our review period.

State has not adhered to established time frames when implementing the commodity jurisdiction process and has been unable to issue determinations for some items due to interagency disputes occurring outside the process. State exceeded the maximum 95 days established in guidance for 62 percent of the jurisdiction determinations made during our review period. Causes for delays included late input from Defense and Commerce, disagreements over the appropriate jurisdiction for an item, need for sufficient information to make determinations, and untimely initial determinations to Defense and Commerce before finalizing an item's jurisdiction. Delays in the process can discourage companies from requesting determinations, as well as affect their ability to compete in certain markets. Additionally, over 30 commodity jurisdictions for space-related items were placed on hold when the National Security Council intervened to resolve a disagreement between Commerce and State. Pending resolution of this disagreement, companies that requested

jurisdiction determinations have exported their space-related items under different controls.

This report contains recommendations to the Secretaries of Commerce, State, and Defense to improve the transparency, consistency, and timeliness of the commodity classification and commodity jurisdiction processes. In commenting on a draft of this report, Commerce disagreed with our findings and conclusions, but it agreed to work with State, Defense, and companies to implement our recommendations. State, in its comments on our draft report, partially concurred with our recommendations. Defense concurred with our recommendations.

Background

The U.S. government's controls on the export of defense-related items are primarily divided between two departments. Commerce, through its Bureau of Industry and Security, controls the export of dual-use items under the authority granted by the Export Administration Act.² Commerce's Export Administration Regulations³ establish the Commerce Control List, which generally contains detailed specifications for dual-use items. State, through its Office of Defense Trade Controls, regulates exports of defense items under the authority of the Arms Export Control Act.⁴ State's International Traffic in Arms Regulations⁵ provide controls over defense items, which are identified in broad categories on the U.S. Munitions List. Both departments' control lists are developed with the Defense Technology Security Administration, which represents Defense on export control issues. Defense reviews both State and Commerce export licenses for national security concerns.

Commerce and State control exports differently in several key areas. Commerce seeks to balance national security, foreign policy, and economic interests when considering how to control items and review export licenses. By contrast, State gives primacy to U.S. national security and foreign policy interests. In most cases, Commerce's controls over

² 50 U.S.C. App. secs. 2401 et seq. Authority granted by the act terminated on August 20, 2001. Executive Order 13222 continues the export control regime established under the act and the Export Administration Regulations.

³ 15 C.F.R. secs. 730-774.

⁴ 22 U.S.C. secs. 2751 et seq.

⁵ 22 C.F.R. secs. 120-130.

dual-use items are less restrictive than State's controls over defense items. State requires licenses for exports and re-exports to all destinations with few exceptions, while many items under Commerce's jurisdiction do not require licenses to most destinations. Also, some sanctions and embargoes only apply to items on the U.S. Munitions List and not to those on the Commerce Control List. For example, most exports of defense items to destinations such as China are prohibited under State, while Commerce can allow the export of many dual-use items to China.

Companies are responsible for determining whether the item they seek to export is on the Commerce Control List and, therefore, subject to Commerce's jurisdiction, or on the U.S. Munitions List and subject to State's jurisdiction. Under Commerce regulations, companies may request a commodity classification when unsure of the requirements for exporting a Commerce-controlled item.⁶ After reviewing the characteristics of the item, Commerce provides an export control classification number from the Commerce Control List, which indicates the applicable controls and licensing requirements.⁷ Under State regulations, companies may request a commodity jurisdiction determination from State when unsure whether an item is subject to State or Commerce controls or when requesting that an item be transferred from State to Commerce jurisdiction.⁸ State is to consult with Defense and Commerce to determine the proper jurisdiction of an item based on several criteria, including its civil applications and military significance. State is the arbiter in the commodity jurisdiction process and is the only department that may change the jurisdiction of an item.

In 1996, the National Security Council issued guidance to improve the transparency and interagency coordination of the commodity classification and commodity jurisdiction processes. The Council's guidance was prompted by State and Commerce disagreement over jurisdictional determinations. This guidance also came after Commerce issued a commodity classification for State-controlled missile technology, which resulted in harm to U.S. national security when this technology was improperly transferred to China. The guidance provides referral criteria

⁶ 15 C.F.R. 748.3.

⁷ Some items may also be designated "EAR99," which serves as a general designation for items that are covered by the Export Administration Regulations but are not specified on the Commerce Control List.

⁸ 22 C.F.R. 120.4.

for when Commerce should consult with State and Defense on commodity classification requests before making a decision. In addition, the guidance establishes time frames for making commodity jurisdiction determinations as well as an interagency dispute resolution process.

Commerce Improperly Classified Items and Has Not Adhered to Regulatory Time Frames

Commerce rarely referred classification requests to State and Defense, even though some items appear to meet referral criteria. Commerce officials said they usually do not obtain input from State and Defense since they have sufficient experience to properly classify items. As a result of the limited referrals, Commerce has improperly classified some State-controlled items as Commerce-controlled. Some of these improper classifications have been identified through the license application review process. However, since many items exported under Commerce do not require licenses to most destinations, the commodity classification process is sometimes the only opportunity for State and Defense to become aware of what companies are exporting. Therefore, other improper classifications may not have been identified. In addition, Commerce has not adhered to regulatory time frames for issuing commodity classifications.

According to the National Security Council guidance, Commerce is to refer to State and Defense all commodity classification requests for “items/technologies specifically designed, developed, configured, adapted and modified for a military application or derived from items/technologies specifically designed, developed, configured, adapted or modified for a military application.” State and Defense can then provide input on whether the items are State-controlled and therefore cannot be classified on the Commerce list or need to be reviewed through the commodity jurisdiction process. The guidance also directs Commerce to promptly forward to State requests from companies asking if an item is under Commerce or State jurisdiction.

Commerce Rarely Referred Classification Requests That Appear to Meet Criteria

Commerce has referred a limited number of commodity classification requests to State and Defense. Of the 12,457 commodity classification requests completed during fiscal years 1998 through 2001, only 40 requests were referred by Commerce to State and Defense for review.⁹ Commerce cited several reasons for referring these cases, including that the items had

⁹ Commerce referred another request in fiscal year 2001 that has not been completed.

military applications or origins, were to be exported to military end-users, or were under State control. Through the referral process the departments agreed that 12 of the requests involved items under State jurisdiction,¹⁰ 9 involved items under Commerce jurisdiction, 18 required additional review through the commodity jurisdiction process, and 1 was withdrawn by the company after it was referred. Commerce did not refer the remaining 12,417 commodity classification requests it completed during this period. Table 1 shows the number of commodity classifications and referrals by fiscal year.

Table 1: Commodity Classifications Completed by Commerce and Referred to State and Defense, Fiscal Years 1998-2001

Fiscal year	Commodity classifications completed	Commodity classifications referred
1998	2,721	6
1999	3,004	5
2000	3,411	12
2001	3,321	17
Total	12,457	40

Source: GAO's analysis of Commerce classification data.

Commerce has based its criteria for referring commodity classification requests to State and Defense on its interpretation of the National Security Council guidance. Commerce officials told us that they follow the guidance to refer classification requests for items specifically designed for military use. For example, Commerce referred a request involving software designed to analyze and simulate submarines. However, under their interpretation of the guidance, Commerce officials do not refer all requests involving items derived from military technology, only those that have been recently adapted for civilian use. For example, Commerce referred a classification request for a military vehicle that was converted for civilian use in the early 1990s. In addition to the guidance, Commerce officials stated they refer requests involving items where jurisdiction is unclear.

In contrast, State and Defense officials said that under their interpretations of the National Security Council guidance, Commerce should be referring most, if not all, commodity classification requests to

¹⁰ One of the requests involved multiple items, most of which were determined to be State-controlled.

them. For example, Defense officials stated that Commerce should refer classification requests for all items derived from military technology regardless of how long ago this occurred. They added that most items on the Commerce Control List were derived from items designed for the military. The officials also stated that Commerce should refer all classification requests involving items with unclear jurisdiction.

Commerce has not consistently applied its referral criteria for implementing the National Security Council guidance. We identified 253 commodity classification requests that appear to meet Commerce's stated criteria for referral but were not referred to State and Defense.

- Commerce returned 123 requests to companies without providing a classification and informed these companies that State should review the items through the commodity jurisdiction process. In other instances, Commerce has referred requests when it needed to confirm which department has jurisdiction over an item.
- Commerce returned 89 requests to companies without providing a classification and informed these companies that the items were subject to State control. By definition, an item that is State-controlled meets the referral criteria of being specifically designed for a military application. Also, Commerce has referred other requests to State and Defense for items it considered to be State-controlled.
- We identified 37 requests involving items that Commerce classified without referral to State and Defense but that are included in categories that appear on both State and Commerce control lists. For example, Commerce provided companies with classifications for two sensitive missile technology items that we had previously identified as subject to unclear jurisdiction since they appear on both Commerce and State's control lists.¹¹
- We found 4 classifications issued by Commerce where the requests were not referred to State and Defense, involving items with military applications, military origins, or unclear jurisdiction—all of which were reasons Commerce cited when referring other requests. For example, one request involved night vision technology, which has military origins and applications and is currently under jurisdictional review by State.

¹¹ See General Accounting Office, *Export Controls: Clarification of Jurisdiction for Missile Technology Items Needed*, [GAO-02-120](#) (Washington, D.C.: Oct. 9, 2001).

Commerce officials stated that the referral criteria are subjective and have not always been applied consistently by Commerce officials that review classification requests. These officials acknowledged that their implementation of the referral criteria may pose some risk of improperly classifying a State-controlled item, but the risk is minimal because Commerce reviewers have sufficient experience with classifying and licensing items. They also stated that increased referrals would limit their ability to meet the regulatory requirement to process commodity classification requests in a timely manner. State and Defense officials told us that they have the necessary expertise to review classification requests to ensure proper jurisdiction. Furthermore, only State, with Defense's concurrence, has been delegated the statutory authority to determine which items are under its jurisdiction.

Commerce does not always receive sufficient information from companies to identify all classification requests that meet referral criteria. Commerce regulations require companies to provide precise technical specifications on an item when submitting a commodity classification request. However, Commerce regulations do not require companies to submit information that relates to referral criteria such as whether an item's applications are predominantly military or civil or whether an item was originally developed for military use. Commerce officials stated that they do not need this information to make classification decisions but would need additional information in some cases to determine whether to refer requests to State and Defense.

Commerce Has Improperly Classified State-Controlled Items and Limited State's Exporter Oversight

Classification of items without input from State and Defense has resulted in Commerce improperly classifying some State-controlled items. We identified several instances in which companies have received classifications from Commerce for State-controlled items without input from State and Defense. For example, one company received classifications for items that can be used to analyze missile flight test data and subsequently submitted several license applications to Commerce to export these items. During its review of the license applications, Defense questioned Commerce's jurisdiction over the items and the company agreed to seek licenses from State to export these items in the future. Two other companies received classifications from Commerce for items containing night vision technology. However, when these companies submitted export license applications to Commerce, Defense objected to Commerce jurisdiction and recommended that the items be licensed through State. Commerce returned one license application to the company because the item may be State-controlled and advised the company to

seek a commodity jurisdiction determination from State. The item in the other license application is currently under jurisdictional review by State.

While Defense officials can identify some improper classifications through the license review process, most Commerce-controlled items do not require export licenses. Therefore, the referral of commodity classification requests could provide State and Defense their only opportunity to become aware of what companies are exporting through Commerce. Of the total classifications provided to companies during fiscal years 1998 through 2001, about two-thirds involved classifications for items that generally would not require export licenses to most destinations. A State-controlled item that is classified as a Commerce item that generally does not require a license can then be improperly exported without the appropriate government review. We identified one company that received a commodity classification for explosive detection devices that would allow the company to export them to most destinations without Commerce licenses. Another company that exports the same devices through State's licensing process notified State of its competitor's activities. This prompted State to issue a commodity jurisdiction determination that the devices are State-controlled. Until this jurisdiction determination was issued, the company obtaining licenses from State experienced a competitive disadvantage because the other company could meet customer demands more quickly by not obtaining licenses.

By not referring classification requests, Commerce also does not provide State with an opportunity to ensure that companies comply with State's governing export control statute and regulations. Pursuant to the Arms Export Control Act,¹² State's regulations require all manufacturers of defense items to register with State, even if they are not planning to export their items.¹³ The U.S. government then uses registration information to ensure compliance with export control laws. Based on our review of classification data, we identified several companies that did not register with State, as required by law, after Commerce advised them that their items were State-controlled. State officials said that they will determine what actions are needed to have these companies comply with the regulations and whether any violations occurred. In addition, a senior State official told us that Commerce's limited referrals and improper classifications may limit State's ability to have enforcement actions taken

¹² 22 U.S.C. sec. 2778(b).

¹³ 22 C.F.R. 122.1.

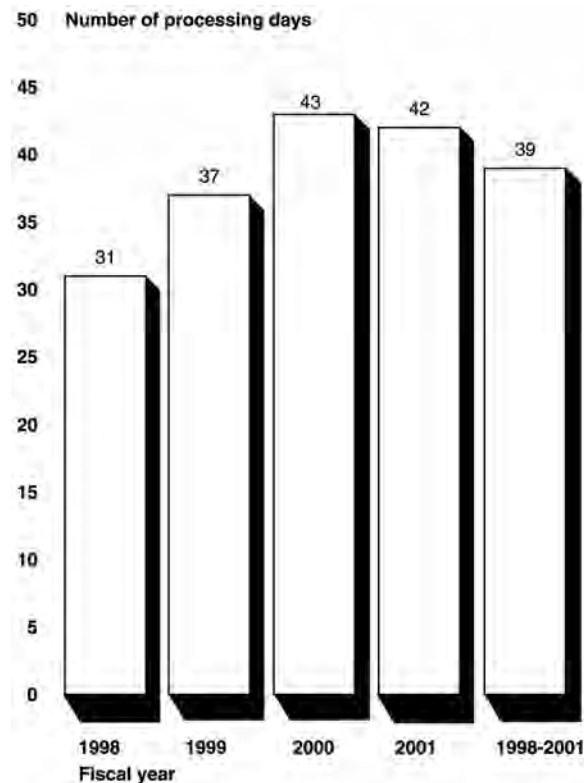
against companies for possible export control violations since the companies have already obtained government direction to export through the Commerce system.

Commerce Has Not Met Required Commodity Classification Time Frames

Commerce has not adhered to regulatory time frames for responding to commodity classification requests from companies. The Export Administration Regulations require Commerce to provide companies with a classification within 14-calendar days.¹⁴ However, during fiscal years 1998 through 2001, Commerce completed only 13 percent of the commodity classifications within 14 days. Commerce took a median of 39 days to respond to classification requests during this 4-year period. Figure 1 shows the median number of days Commerce took to respond to classification requests by fiscal year.

¹⁴ 15 C.F.R. 750.2.

Figure 1: Median Processing Times for Commodity Classifications, Fiscal Years 1998-2001



Source: GAO's analysis of Commerce classification data.

Commerce officials stated that delays in responding to classification requests are due to other priorities, limited staff resources, and companies not providing required information. Commerce officials, who review commodity classification requests, assign highest priority to processing licenses because companies rely on the timely issuance of licenses to meet customers' orders. These officials have other duties that delay their review of classification requests, which include providing information for enforcement cases. Commerce officials noted that they recently received additional hiring authority for personnel to review commodity classification requests and perform other duties, but they have not yet completed the hiring process. Commerce officials also attributed delays to companies not providing required technical specifications with their commodity classification requests, estimating that about 80 percent of requests require officials to perform additional research. If companies provided the required information, then Commerce could spend less time

processing each commodity classification request. Commerce officials told us that they have implemented a new procedure to place requests on hold while they obtain additional information from companies, thereby reflecting Commerce's actual processing time.

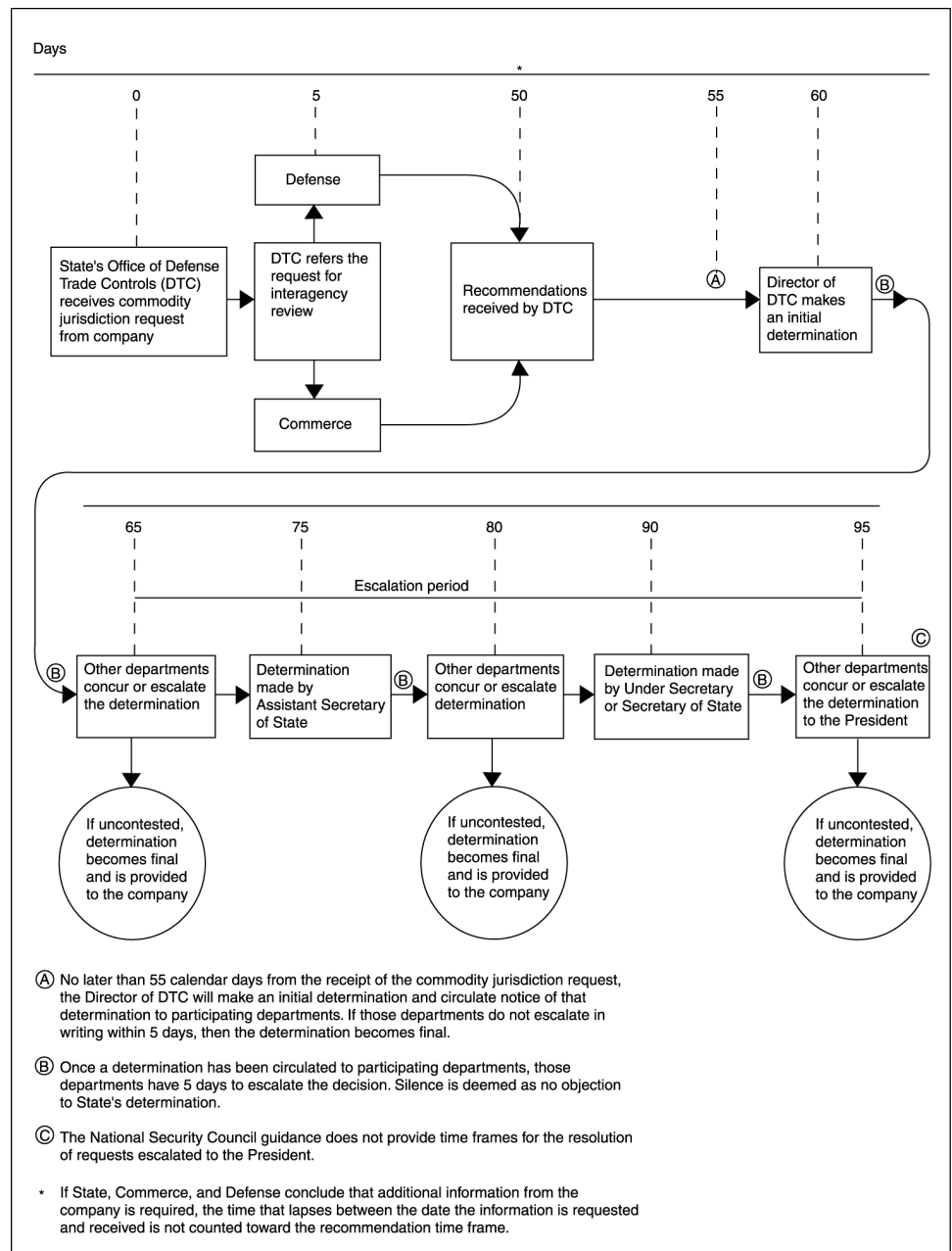
Commodity Jurisdiction Process Exceeded Time Frames and Is Affected by External Disagreements

The commodity jurisdiction process has exceeded established time frames and is affected by external disagreements. State has often not adhered to the 95-day time frame established by the National Security Council for providing companies with commodity jurisdiction determinations. Factors that delay determinations have included late input from Defense and Commerce, disagreements among the departments over the appropriate jurisdiction for an item, need for sufficient information to make determinations, and initial determinations to Defense and Commerce not issued in accordance with guidance. Delays in resolving jurisdiction requests can discourage a company from using the process and affect its ability to compete in certain markets. In addition, an interagency disagreement being resolved outside the commodity jurisdiction process has affected the resolution of some requests.

According to the National Security Council guidance, all commodity jurisdiction requests are to be resolved through a State-led process within a maximum 95-calendar day time frame. During that period, State refers requests to Commerce and Defense, providing them up to 45 days to recommend the appropriate jurisdiction for an item.¹⁵ State is also to resolve any disagreements over jurisdiction between the departments and issue a determination to the company. If the departments disagree on the appropriate jurisdiction for an item, they can escalate initial jurisdiction determinations to higher levels within State and ultimately to the President. Figure 2 shows each step in the commodity jurisdiction process and the associated time frames for issuing determinations.

¹⁵ The National Security Council guidance indicates that Commerce and Defense should provide their recommendations within 35 calendar days, but they may request 10 additional days to submit recommendations for extraordinary cases.

Figure 2: Commodity Jurisdiction Process and Time Frames

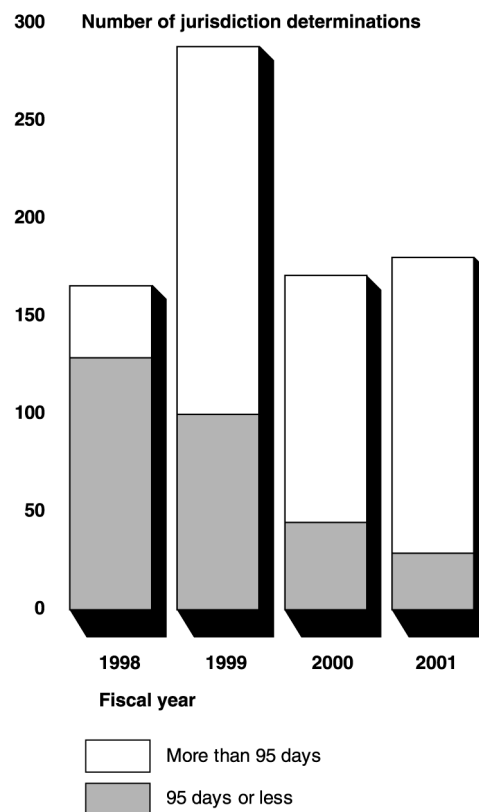


Source: Based on National Security Council guidance.

Commodity Jurisdiction Determinations Have Not Been Timely

State has not adhered to the time frames established in guidance for responding to commodity jurisdiction requests. Of the 802 commodity jurisdiction determinations made by State between October 1, 1997, and May 31, 2001, 62 percent took over the maximum 95 days to resolve.¹⁶ State took a median of 118 days to issue a jurisdiction determination, with 25 percent taking twice as long as the established maximum time frame. Figure 3 shows the total number of determinations and those that took over 95 days to resolve by fiscal year.

Figure 3: Commodity Jurisdiction Determinations and Timeliness, Fiscal Years 1998-2001



Note: Fiscal year 2001 includes only those cases resolved by May 31, 2001.

Source: GAO's analysis of State commodity jurisdiction data.

¹⁶ We requested data on jurisdiction determinations made during fiscal years 1998 through 2001. However, State only provided data on determinations made from fiscal year 1998 through May 31, 2001.

While State consistently referred jurisdiction requests to Defense and Commerce in a timely manner, State has not adhered to established time frames for issuing commodity jurisdiction determinations generally due to four contributing factors. First, for the majority of determinations made between October 1, 1997, and May 31, 2001, Commerce and Defense did not provide their recommendations on the appropriate jurisdiction within 45 calendar days. Specifically, Commerce took a median of 81 days while Defense took 69 days to provide State with their respective recommendations. State officials explained that they are reluctant to make jurisdictional determinations without input from the other departments, particularly since Defense has a statutory role in developing the U.S. Munitions List. Defense and Commerce officials told us they are sometimes late because commodity jurisdictions are low priority. According to these officials, their limited staff resources are primarily devoted to reviewing export license applications. For example, during our review period, Defense had one official responsible for administering the commodity jurisdiction process and coordinating input from technical experts, but it has recently hired an additional staff person. Additional time may be needed for the departments to provide their recommendations in certain cases. For 3 of the 34 commodity jurisdiction files we reviewed, Defense officials requested additional time to provide their recommendations, citing either internal disagreements about the appropriate jurisdiction or the precedent setting nature of the case.

Second, State's ability to resolve jurisdiction requests has been delayed by disagreements between the departments over the appropriate jurisdiction for an item. When Commerce and Defense both provided recommendations to State, they conflicted 35 percent of the time. In such cases, State took a median of 51 additional days to issue a determination. According to State officials, they attempted to reconcile the departments' positions by discussing the cases with the departments and conducting further research on the military applications and origins of the item. In one of the commodity jurisdiction files we reviewed where there was disagreement between the departments, State indicated that it was suspending the established time frame because the case was complex.

Third, the issuance of commodity jurisdiction determinations has been delayed by the need for sufficient information. In some instances, State officials told us that they have not always found the information and justifications from Commerce to be sufficient for them to make determinations. In several of the commodity jurisdiction files we reviewed, Commerce did not fully address whether the items have predominate civil applications or performance equivalents to those used in civil applications,

which are among the criteria State uses when determining jurisdiction. According to Commerce and State officials, Commerce has recently improved the quality of input to State. Furthermore, State officials told us they need to conduct additional research on an item before making a determination, regardless of the quality of input from Commerce and Defense.

Fourth, State has not always issued initial determinations in accordance with the guidance. State is to provide Commerce and Defense with initial jurisdiction determinations no later than 55 calendar days after receiving a request, even when those departments have not provided their input. If Commerce and Defense do not object within 5 days, State's decision becomes final. According to Commerce and Defense officials, commodity jurisdictions become a priority when they receive State's initial determinations, so they can provide input before the determinations become final. A senior State official told us that State would prefer to receive Commerce and Defense's input as set out in the guidance before issuing an initial determination. Our review of commodity jurisdiction files indicated that most did not contain documentation on initial determinations. Those files that did contain documentation indicated that State issued initial determinations more than 75 days after receiving the request. Additionally, State has not tracked the issuance of initial determinations in its commodity jurisdiction database.

While the commodity jurisdiction process is used to assist companies, State's delays may discourage companies from requesting jurisdiction determinations. For example, officials from two companies told us that they are reluctant to request determinations in the future because of delays they have experienced in the process. Officials with other companies expressed dissatisfaction with the process because they were unable to obtain information from State on the status of their pending requests. Therefore, companies may determine jurisdiction on their own or seek jurisdiction guidance outside the process.

Delays in the commodity jurisdiction process may also affect a company's ability to compete in certain markets. An item is generally subject to State's export controls until State determines otherwise. As a result, pending the resolution of a commodity jurisdiction request, the item is subject to State's restrictions and generally requires a license to be exported. Under current U.S. law, most items subject to State's jurisdiction

cannot be licensed for export to China.¹⁷ Commerce does not have a comparable restriction on the export of dual-use items to China. For example, officials with one company informed us that they were unable to compete for a significant contract in China while waiting over a year for a commodity jurisdiction determination. State eventually determined that the item in question was subject to Commerce's jurisdiction, which it did in 36 percent of the cases resolved during our review period. Officials with other companies also stated that delays in receiving jurisdiction determinations have affected their ability to compete in certain markets.

Interagency Disagreement Outside the Process Affects Resolution of Some Commodity Jurisdiction Requests

Commodity jurisdiction requests for space-related items have remained unresolved for several years due to an interagency jurisdictional debate occurring outside the established commodity jurisdiction process. In March 1999, State and Commerce issued regulations pursuant to a change in law that transferred commercial satellites and related items from Commerce's jurisdiction to State's jurisdiction.¹⁸ Commerce and State disagreed on what constituted "related items" and whether the law transferred certain space-related items to State. The National Security Council initiated an interagency review to resolve the disagreement and determine jurisdiction over these items. At the direction of the National Security Council, State placed commodity jurisdiction cases for space-related items on hold until an interagency agreement could be reached and implemented. As a result, State officials said they placed 33 commodity jurisdiction cases on hold, most of which have been open since 1999. In 2001, State and Commerce announced the resolution of the disagreement, and they are currently developing regulations to specify control over these items.

While their commodity jurisdiction requests remain on hold, companies have exported their space-related items through both departments. Officials with four companies told us that they have been exporting their space-related items through State. Officials with another company told us, that based on advice from Commerce, they have been exporting their space-related items through Commerce. State and Commerce officials confirmed that companies could export such items through Commerce.

¹⁷ P.L. 101-246, Feb. 16, 1990. Under the statute, licensing of State-controlled items for export to China is prohibited unless the President reports to Congress that (1) China has achieved certain political and human rights reforms or (2) it is in the U.S. national interest.

¹⁸ P.L. 105-261, Oct. 17, 1998.

However, neither department issued written guidance specifying what companies with pending commodity jurisdiction requests should do.

While the origins of the jurisdictional disagreement over space-related items were unique, disagreements between departments over the jurisdiction of other items could limit State's ability to make determinations through the commodity jurisdiction process. For example, State has placed a jurisdiction request involving night vision technology on hold until jurisdiction for that technology is decided through the ongoing review of the U.S. Munitions List.¹⁹ State officials said they expect this review of night vision technology to be difficult and time-consuming to complete. Defense and Commerce officials also told us that there is considerable interagency debate on how night vision technology should be controlled.

Conclusions

The bifurcated U.S. export control system seeks to manage risks by balancing national security and foreign policy with economic interests. Commerce has altered this balance by not implementing the commodity classification process in a manner that considers other stakeholder interests. While State's implementation of the commodity jurisdiction process allows for the consideration of multiple interests, it is slow to reach decisions and, in some cases, has been affected by larger interagency disputes occurring outside of the process. Existing guidance was intended to improve transparency and coordination within these processes, but problems persist. If the U.S. export control system is to effectively manage risk, these processes have to balance stakeholder interests, be transparent to stakeholders, and efficiently reach and communicate decisions. In the absence of this, the U.S. government faces the possibility of defense-related items being exported without the proper level of government review and control to protect national interests. Also, companies may export similar items under different controls, placing some companies at a competitive disadvantage or at risk of violating U.S. export control laws.

¹⁹ State and Defense are reviewing and revising different portions of the U.S. Munitions List on an annual basis, as part of the Defense Trade Security Initiative, to ensure that coverage on the list is appropriate. See General Accounting Office, *Defense Trade: Analysis of Support for Recent Initiatives*, [GAO/NSIAD-00-191](#) (Washington, D.C.: Aug. 31, 2000).

Recommendations for Executive Action

To increase transparency to stakeholders and minimize the risk of Commerce making jurisdictional determinations through the commodity classification process, we recommend that the Secretary of Commerce direct the Bureau of Industry and Security to promptly review existing guidance and develop, with the concurrence of the appropriate entities within State and Defense, criteria for referring commodity classification requests to those departments. In developing the criteria, the departments should agree on a common definition of terms to be contained in the criteria. Until the departments develop and implement referral criteria, the risk of Commerce improperly classifying State-controlled items will continue to exist.

To increase transparency and assist State in enforcing its statutory requirements, we recommend that the Secretary of Commerce direct the Bureau of Industry and Security to develop, with the concurrence of State's Office of Defense Trade Controls, procedures for referring requests that are returned to companies because the items are State-controlled or require a commodity jurisdiction review.

To ensure that Commerce has sufficient information to make timely and appropriate commodity classifications, we recommend that the Secretary of Commerce direct the Bureau of Industry and Security to revise guidance for companies on the information to be provided with commodity classification requests and consider including a requirement for information on an item's origins and applications.

To comply with existing time frames for responding to classification requests, we recommend that the Secretary of Commerce direct the Bureau of Industry and Security to assess the amount of resources needed, then reallocate resources as appropriate.

To improve the timeliness of the commodity jurisdiction process, we recommend that the Secretaries of State, Commerce, and Defense direct the respective entities within their departments to assess the amount of resources needed to make jurisdiction recommendations and determinations within established time frames, then either reallocate resources as appropriate or seek changes to the established time frames that are consistent with available resources. We also recommend that the Secretary of State direct the Office of Defense Trade Controls to issue initial determinations in accordance with the guidance.

To improve transparency and consistency of the commodity classification and jurisdiction processes, we recommend that the Secretaries of State,

Commerce, and Defense revise interagency guidance to incorporate any changes to the referral process and time frames for making decisions.

Agency Comments and Our Evaluation

We received written comments on a draft of this report from Commerce, State, and Defense, which are reprinted in appendixes I, II, and III, respectively, along with our detailed evaluation of their comments. Commerce disagreed with our findings and conclusions, which it believes are based on erroneous facts and, therefore, are fundamentally flawed. Specifically, Commerce did not agree with our finding that 253 classification requests, which were not referred, appear to meet Commerce's referral criteria and, therefore, should have been referred. Commerce asserts that it did not improperly classify State-controlled items. Additionally, Commerce indicated that State and Defense's position that most commodity classifications should be referred does not reflect the National Security Council guidance. However, Commerce agreed to work with other departments and companies to implement our recommendations and noted it has allocated resources to ensure the timely issuance of its classifications and State's jurisdiction determinations. In responding to our draft, State partially concurred with our findings and recommendations. State noted that it has made progress in reducing the amount of time needed to issue jurisdiction determinations. Citing improved timeliness and deference to Defense's national security views, State did not agree that it needs to implement our recommendation to issue initial determinations in a timely manner, but it did agree to enlist greater cooperation from other departments in meeting established time frames. In its comments, Defense concurred with our recommendations.

We disagree with Commerce's characterization of our findings and conclusions and are confident that our report accurately assesses Commerce's implementation of the commodity classification process. As stated in our report, we identified at least 253 classification requests that appear to meet the referral criteria. By Commerce's own admission, requests involving State-controlled items or those in need of a jurisdictional review were returned to the companies without referral to State and Defense, which is not consistent with the referral criteria. In addition, Commerce inconsistently applied the criteria because in some instances it referred requests that met the criteria. Our report highlights the risk of Commerce improperly classifying State-controlled items through the commodity classification process. We identified several instances in which Commerce classified State-controlled items, including explosive detection devices that were determined to be State-controlled through the commodity jurisdiction process. Commerce's position

regarding the interpretation of the National Security Council guidance by State and Defense demonstrates that the criteria are subjective and that the departments have not reached a consensus on which requests should be referred. While we cannot verify whether State has decreased the amount of time needed to process jurisdiction requests, we agree that State should enlist the cooperation of other departments to improve timeliness. We continue to recommend that State issue initial determinations in accordance with established guidance because this is a mechanism to improve timeliness, while still providing Defense and Commerce with an opportunity to provide input before a final determination is made.

Scope and Methodology

To assess how Commerce implements the commodity classification process, we reviewed relevant laws, regulations, and the National Security Council guidance to identify the criteria for the process and examined how Commerce implemented the criteria. We discussed the process and the referral criteria with officials from Commerce's Bureau of Industry and Security, State's Office of Defense Trade Controls, and Defense's Defense Technology Security Administration. We reviewed 41 commodity classification requests Commerce referred to State and Defense during fiscal years 1998 through 2001 and identified the reasons for referral. We analyzed commodity classification data for fiscal years 1998 through 2001 and selected 34 cases to review that were not referred to State and Defense. We compared the characteristics of the items in the 34 cases with Commerce's stated referral criteria, as well as items identified as State-controlled in Defense's review of Commerce licenses. We reviewed the data and identified nonreferred requests returned to companies without classifications because the items either were State-controlled or needed a commodity jurisdiction review. We then confirmed whether the companies involved in these cases appeared in State's registration database. In addition, we reviewed the classification data to identify the export control classification numbers provided to companies. We then compared those classification numbers with classification numbers that cover items appearing on both the Commerce and State control lists. To determine Commerce's timeliness in providing classifications, we analyzed the time elapsed between the receipt of the classification request and the issuance of the classification. To assess the reliability of Commerce's classification data, we compared information in selected files to the data. During our analysis, we found some minor inaccuracies with Commerce's data, which did not adversely affect its overall reliability.

To assess how State implements the commodity jurisdiction process, we identified the steps in the commodity jurisdiction process as established in relevant regulations and the National Security Council guidance and discussed the implementation of the process with officials from the relevant offices at State, Defense, and Commerce. We requested State's data for commodity jurisdiction determinations and open cases during fiscal years 1998 through 2001. However, State did not provide complete data for fiscal year 2001. We analyzed the data to determine the time taken to complete key steps in the process. We reviewed 34 selected commodity jurisdiction files. We discussed reasons for delays as well as the interagency disagreement over space-related items with State, Commerce, and Defense officials. We also reviewed documents related to the history of the space-related interagency disagreement. To assess the reliability of State's commodity jurisdiction data, we compared the information in the files reviewed to the data and found inconsistencies. However, we determined that these are the best available data and are sufficiently reliable for assessing timeliness.

We discussed the commodity classification and jurisdiction processes with companies. To select companies, we analyzed Commerce and State data to identify companies that had experience with one or both processes. We also obtained recommendations from industry associations and others to develop a list of additional companies that had used these processes. We then conducted structured interviews with officials from 31 companies, which included small, medium, and large companies with varying degrees of experience in using the export control processes.

We conducted our work from May 2001 through September 2002 in accordance with generally accepted government auditing standards. The time taken by State, Commerce, and Defense to respond to our requests for information and data adversely affected the timeliness of our reporting.

We will send copies of this report to the Chairmen and Ranking Minority Members of the House Committees on Government Reform, on International Relations, and on Armed Services and Senate Committees on Governmental Affairs, on Foreign Relations, on Armed Services, and on Banking, Housing, and Urban Affairs. We will also send copies to the Secretaries of State, Commerce, and Defense; the Director, Office of Management and Budget; and the Assistant to the President for National Security Affairs. In addition, this report will be made available at no charge on the GAO Web site at <http://www.gao.gov>.

If you or your staff have questions concerning this report, please contact me at (202) 512-4841. Others making key contributions to this report are listed in appendix IV.

Sincerely yours,

A handwritten signature in black ink, reading "Katherine V. Schinasi". The signature is written in a cursive style with a large, stylized initial "K".

Katherine V. Schinasi
Director, Acquisition and Sourcing Management

Appendix I: Comments from the Department of Commerce

Note: GAO comments supplementing those in the report text appear at the end of this appendix.



UNITED STATES DEPARTMENT OF COMMERCE
Bureau of Industry and Security

Washington, D.C. 20230
September 9, 2002

Ms. Katherine V. Schinasi
Director, Acquisition and Sourcing Management
United States General Accounting Office
Washington, D.C. 20548

Dear Ms. Schinasi:

Thank you for the opportunity to comment on the draft General Accounting Office (GAO) report titled EXPORT CONTROLS: Processes for Determining Proper Control of Defense-Related Items Need Improvement.

The report reaches two principal conclusions with respect to the Commerce Department's commodity classification practices: (1) that the Commerce Department has failed to refer to the Departments of State and Defense certain commodity classification requests received from exporters during the period 1998-2001 that should have been referred, consistent with guidance issued by the National Security Council (NSC) in 1996, and (2) that, "as a result of the limited referrals, Commerce has improperly classified some State-controlled items as Commerce-controlled." We believe that both conclusions are based on erroneous facts and, therefore are fundamentally flawed.

The report's conclusions are all premised on the GAO's identification of 253 (out of over 12,000) commodity classification requests that the Commerce Department received that the GAO believes, "appear to meet Commerce's referral criteria" but that the Commerce Department did not refer. Commerce Department staff has reviewed these 253 requests. It turns out that in 212 of these cases Commerce did not issue the requester a commodity classification at all, but instead referred the requester to the State Department. With respect to the remaining, 41 cases – more accurately, 39 cases, as the GAO appears to have double-counted two cases – the report provides a superficial explanation of why the GAO believes referral was merited in those cases or how the products in those cases were classified incorrectly. In fact, after review, we have determined that those 39 requests did not require referral under either the 1996 NSC guidance or the Commerce Department's own criteria. Moreover, those 39 requests were, in any event, classified correctly.

To be sure, there may be differences among the agencies as to what ideally the referral practice should be with respect to commodity classification requests. The report itself cites unnamed representatives of the Departments of State and Defense who believe that the Commerce Department "should be referring most, if not all, commodity classifications to them." Whatever the potential merits of such a broad referral policy (which would likely entail substantial lengthening of the classification process with concomitant economic costs), this approach clearly does not reflect the guidance set forth by the NSC in 1996 and should not be used as the benchmark against which to judge Commerce Department practices.



See comment 1.

**Appendix I: Comments from the Department
of Commerce**

Ms. Katherine V. Schinasi
Page 2

For the reasons stated above, we would urge that, prior to finalization of this report, the GAO meet with Commerce Department technical experts and clarify misunderstandings regarding the classification requests that purportedly form the basis of the report's conclusions. More detailed comments on the report are attached.

Sincerely,



Matthew S. Borman
Deputy Assistant Secretary

Attachment

**Appendix I: Comments from the Department
of Commerce****Department of Commerce Comments on the Draft GAO Report
EXPORT CONTROLS: Processes for Determining Proper Control
of Defense-Related Items Need Improvement
(GAO Code 120062)****GENERAL COMMENTS**

See comment 1.

1. The Report's Conclusions about Commerce's Classification Processes Are Fundamentally Flawed because They Are Based on Erroneous Facts. The Report's conclusions are premised on its assertion that during the period 1998-2001, the Commerce Department failed to refer to other agencies 253 commodity classification requests that should have been referred. The Report states that, "as a result of the limited referrals, the Commerce Department has improperly classified some State-controlled items as Commerce-controlled."

We have reviewed the 253 classification requests identified by the GAO and believe that they do not support the GAO's conclusions. 212 of the 253 requests identified by the GAO never resulted in the issuance of a classification by the Commerce Department at all and, therefore, could not have been "improperly classified" by Commerce. Rather, upon an initial review of these classification requests, the requests were returned to the applicants and the applicants were referred directly to the State Department.¹

See comment 2.

We have determined that the 41 remaining cases (which are in fact only 39 cases because the GAO "double counted" two of the cases) did result in issuance of a commodity classification but did not require referral to the other agencies. The GAO's premise for believing that these requests should have been referred was apparently that the items at issue in those requests appear to be covered by both the U.S. Munitions List (USML) and the Commerce Control List (CCL). However, as the Commerce Department noted in response to a previous GAO report (GAO Code 707550), the fact that an item might appear to be covered by both the USML and the CCL does not necessarily mean that jurisdiction over the item is unclear (and thus that a referral is required). The CCL describes – in far greater specificity than the USML – relevant technical control parameters agreed upon by the Departments of Commerce, State, and Defense. An item that meets those parameters is not on the USML by interagency agreement. For example, one of the non-referred classifications that the GAO identified was for AFLATOXIN. Although toxins

¹ Classification requests that clearly involve items specifically designed, developed, configured, adapted, or modified for a military application are returned to the exporter without action and with instructions that the exporter consult with the State Department. It is not necessary to consult with the Departments of State or Defense when it is clear that the Commerce Department does *not* have jurisdiction. In these cases, the applicant is directed to the Department of State. Putting such cases into the referral process would likely prolong the process for the exporter and needlessly consume limited government resources. It remains the exporter's responsibility to comply with all export laws, regardless of whether the Commerce Department or the State Department has jurisdiction.

**Appendix I: Comments from the Department
of Commerce**

See comment 3.

See comment 4.

that fall outside the CCL control parameters might be covered by the USML, this toxin is clearly on the CCL (Export Control Classification Number (ECCN) 1C351.d.1 1). This item, therefore, is not under State jurisdiction and did not require referral.

In any event, we have reviewed the 39 remaining cases and determined that they were correctly classified because they all clearly fell within the relevant CCL entries. The GAO's report provides no evidence to the contrary².

2. The Report Erroneously Faults Commerce for "Rarely" Referring Commodity Classification Requests. As noted above, the Report's conclusion – that the Commerce Department did not refer classification requests that it should have – is fundamentally erroneous. More generally, the Report suggests that the Commerce Department refers classification requests too "rarely." In fact, the Commerce Department refers inter-agency those requests that it is required to refer under the National Security Council's (NSC) 1996 Guidance.

The NSC Guidance provides that the Commerce Department will share commodity classification requests with the Departments of State and Defense for items specifically designed, developed, configured, adapted, or modified for a military application, or derived from items specifically designed, developed, configured, adapted, or modified for a military application. These criteria define a narrow category of items and clearly belie the assertions of representatives of State and Defense, as provided in the Report, that the Commerce Department "should be referring most, if not all, commodity classifications to them."

The dual-use export control system administered by the Commerce Department is broad in scope – covering all items in the U.S. economy, except items specifically under the jurisdiction of other Departments. Commodity classification requests cover the full range of these items. With respect to many of these requests, there is no issue about the item potentially being "designed . . . for a military application" or "modified for a military application," and thus subject to referral under the NSC Guidance. Rather, these requests concern whether an item is appropriately classified under one CCL sub-category or another. Accordingly, it is appropriate that Commerce Department referrals be relatively "rare."³

See comment 5.

To be sure, the NSC Guidance could be interpreted in such an awkward fashion as to merit referral of a larger array of commodity classification requests. For example, a product such as the *Barbie Chat With Me* walkie talkie could require referral because the first portable FM two-

² The GAO Report also made reference to an additional four cases that will be discussed later in these comments.

³ It should be noted that, even if GAO were correct about the 253 requests discussed above (which it is not), Commerce Department referrals would still be relatively rare – i.e., they would occur in approximately 2 percent of the cases.

**Appendix I: Comments from the Department
of Commerce**

way radio was originally designed by Motorola for the U.S. Army Signal Corps in 1940. This is not how the NSC Guidance has been traditionally interpreted, and such an interpretation would result in inefficient use of scarce government resources and an unnecessary burden on U.S. exporters.

See comment 6.

3. The Report Fails to Evaluate Compliance with All NSC-Mandated Referral Processes.

Although the Report reviews Commerce Department referral and classification decisions under the 1996 NSC guidance, it does not evaluate implementation of the reciprocal NSC requirement that the State Department refer certain munitions license applications to the Commerce Department for review. Since 1996, the Commerce Department has received only one informal referral of a munitions license from the State Department. The Report also fails to evaluate whether jurisdictional decisions by the State Department or jurisdictional assertions by the Defense Department are consistent with jurisdictional criteria set forth in the International Traffic in Arms Regulations (ITAR). If incorrect, such decisions could adversely affect U.S. economic welfare, and could also can skew perceptions of what types of items appropriately merit commodity classification referrals.

See comment 7.

4. The Report Fails to Recognize the Nature of Commodity Classification Determinations.

Commodity classification requests are not licensing determinations. Rather, they are objective, determinations as to whether an item meets the technical parameters of a specific ECCN. The Report fails to note that the Commerce Department officials responsible for commodity classifications are seasoned engineers with experience in industry and the military. Commerce Department engineers have the ability to properly evaluate the technical specifications of a commodity and match those specifications to one of the detailed ECCN entries on the CCL. It is also important to note that the ITAR does not define what is meant by specifically designed, developed, configured, adapted, or modified for a military application.

See comment 8.

5. Commerce Cannot Confirm GAO's Assertions regarding Median Processing Times for Commodity Jurisdiction Cases. The Commerce Department is unable to verify the GAO's assertions regarding the median processing time of the Commerce Department for commodity jurisdiction responses to State. The Commerce Department does not have access to data used by the GAO for its review. We would note, however, that the data should exclude the time the case was not under the Commerce Department's control (i.e., the time between the Commerce Department's initial response and when the Commerce Department might reopen the case to appeal the State Department's initial determination); otherwise, the median processing time will be overstated. We would further note that the amount of time between the Commerce Department's initial recommendation and the State Department's initial determination is considerable. For example, on one commodity jurisdiction case, the Commerce Department provided its initial response to the State Department on November 6, 2000, and reopened the case on February 15, 2001 to appeal the State Department's initial determination. Because the Commerce Department's electronic database used to track these cases is old and relatively unsophisticated, it shows the Commerce Department as taking 126 days to process this case.

See comment 9.

**Appendix I: Comments from the Department
of Commerce**

This figure represents the number of days from initial referral to the Commerce Department until the Commerce Department's appeal of State Department's initial determination was completed. This number is far greater than the actual number of days the Commerce Department had the case. For this case, the Commerce Department's actual review time was 24 days; the State Department's was 102 days. This limitation will be addressed in the redesign of the Commerce Department's Export Control Classification System (ECASS); however, it is an important characteristic for the GAO to note in calculating median processing time.

SPECIFIC COMMENTS**Page 2**

As noted above, the Commerce Department disagrees with the assertion that it has improperly classified some State-controlled items. The Commerce Department also disagrees that 253 that were not referred commodity classification requests appear to meet the referral criteria.

Regarding classification processing times, the Commerce Department is taking several steps to reduce such times, including hiring additional engineers (six in fiscal year 2002 and an additional four, if the budget request is appropriated, in fiscal year 2003), implementing the ability to place commodity classifications on hold without action status in ECASS while licensing analysts wait for additional information from the exporter, and improving the electronic commodity classification system as part of the ECASS upgrade.

As noted above, the Commerce Department cannot evaluate GAO's calculation of our median processing time for commodity jurisdiction requests. For commodity jurisdiction requests for space qualified items, the Department of Commerce, State, and Defense have reached agreement on this issue. The Departments of Commerce and State will be issuing implementing rules soon.

Page 3

It should be noted that the export control system administered by the Commerce Department has considerable input from the Department of State and the Department of Defense, which clear on all substantive changes to the Export Administration Regulations (EAR), including changes to the CCL. Under Executive Order 12981, as amended, those Departments can make recommendations on all license applications submitted to the Commerce Department.

Page 4

On the specific case referenced, jurisdiction on the specific technical data at issue was not clearly delineated in the EAR and the ITAR.

See comment 10.

See comment 11.

See comment 12.

**Appendix I: Comments from the Department
of Commerce**

See comment 13.

Page 5

As noted above, the Commerce Department disagrees that it has improperly classified items. The GAO has only one example of a case in which it alleges the Commerce Department classified an item as on the CCL and the State Department subsequently issued an inconsistent commodity jurisdiction determination. However, the GAO refused to provide the Commerce Department any information on this case; thus, the Commerce Department cannot evaluate the GAO's assertion. The Commerce Department notes that when this item was placed on the CCL, through an interagency cleared rule, there was no corresponding change to the USML. The GAO also failed to review whether the State Department's determination comported with the USML criteria set forth in the ITAR.

Page 6

Regarding the classification request for a military vehicle converted for civilian use, it should be noted that this involves the civil derivative of that vehicle. The Commerce Department properly referred this request because it was not for the finished vehicle (which has been classified under the EAR for nearly 10 years), but rather for the frame and power transfer systems which have a higher percentage of commonality between the civil and the military versions of the vehicle.

See comment 14.

As noted above, the notion that most, if not all, classifications should be referred to the Departments of State and Defense is inconsistent with the scope and establishment of the CCL and Commerce Department jurisdiction.

Pages 7-10

See comment 15.

In addition to the 253 licenses referenced above, GAO also discusses "several" non-referred classifications that it claims were improperly classified (page 8 of the Report). Despite Commerce Department requests, GAO refused to provide either the classification numbers or the related license application numbers for these cases. As a result, the Commerce Department is unable to address in detail GAO's assertions. Nonetheless, several comments can be made based on the information in the Report. First, if the State Department or the Defense Department raise a jurisdictional claim in processing a license application submitted to the Commerce Department, the application generally must be returned without action to the exporter to apply for a commodity jurisdiction determination from the State Department. Returning such applications to the applicant does not reflect agreement by the Commerce Department that the item may be on the USML. Rather, it reflects the practical reality that the application cannot be further processed without a commodity jurisdiction determination. Second, for the four classifications noted on page 7 of the Report, three of which involved night vision equipment, there is an interagency MOU on night vision items that the Commerce Department applies to such commodity classifications. In the case of the explosive detection devices covered under ECCN 2A993 (page 7 and 9), this CCL control was approved interagency, but there was no counterpart revision of the USML. Classifications for such items were likely proper under existing guidelines. The

**Appendix I: Comments from the Department
of Commerce**

See comment 16.

Commerce Department also notes that GAO did not discuss any of these cases with Commerce Department technical experts during this review. Such a discussion would have led to a better informed analysis of these cases.

Also see above comments on steps the Commerce Department is taking to improve the timeliness of its classifications. Specific to Commerce Department actions having an impact on State Department enforcement actions, the Commerce Department fails to see how returning classification requests to applicants and informing them to contact State could affect enforcement actions. If anything, Commerce Department responses should strengthen enforcement cases by putting companies on notice to contact the State Department.

Page 15

See above comments on Commerce Department commodity jurisdiction processing times.

Page 18

See comment 17.

The Commerce Department has not altered the balance of the dual-use export control system. Even by GAO's calculations, only a very small percentage of classification requests would be referred to the Departments of State and Defense. Not considering the cases for which the Commerce Department told applicants to contact the State Department, the number of cases identified is less than one-third of 1 percent. This hardly represents an altering of the balance. Moreover, of the cases GAO identified to the Commerce Department, our review indicates these classifications were properly not referred and properly classified based on the interagency cleared criteria in the EAR. Consequently, although improvements can be made to the classification review system, it does not represent a risk to national security. Regarding the impact on industry, the Commerce Department notes that GAO failed to review how the Departments of State and Defense apply the ITAR criteria for USML items and State Department's sharing of munitions license applications with the Commerce Department under the NSC guidance.

COMMENTS ON GAO'S RECOMMENDATIONS

See comment 18.

As set forth above, the Commerce Department believes that the draft report is fundamentally flawed with respect to its conclusions concerning the Commerce Department's commodity classification processes, and urges further consultation between GAO and the Department before finalizing the study. Such further consultation may affect the GAO's recommendations. In the event that GAO decides not to seek further consultation, we offer the following comments on the recommendations provided.

Recommendation: *Promptly review existing guidance and develop, with the concurrence of the appropriate entities within State and Defense, criteria for referring commodity classification requests to those departments.*

**Appendix I: Comments from the Department
of Commerce**

- Comment: The Commerce Department supports an interagency review of the NSC guidance, including referral of munitions license applications and application of the ITAR criteria for the USML, to address any misperception that the Commerce Department does not refer enough classifications.
- Recommendation: *Develop with the concurrence of State's Office of Defense Trade Controls, procedures for referring requests that are returned to companies because the items are State-controlled or require a commodity jurisdiction review.*
- Comment: The Commerce Department will discuss this recommendation with the State Department to determine the most effective way to address this issue.
- Recommendation: *Revise guidance for companies on the information to be provided with commodity classification requests and consider including a requirement for information on an item's origins and applications.*
- Comment: The Commerce Department will solicit public comment on this recommendation. Note that the EAR provides exporters detailed guidance in Section 748.3 and Supplement No.1 to part 748 on the correct way to submit classification requests and the type of information needed to conduct a technical analysis. On GAO's suggestion that exporters should be required to provide information on an item's origin and applications, exporters are currently required to provide the name of the manufacturer, if known, and a technical description of the items. Applying this recommendation too broadly could have the unintended consequence of catching clearly commercial items, such as the toy described above.
- Recommendation: *Assess the amount of resources needed to comply with the regulations, then either reallocate resources as appropriate or make a regulatory change that reflects a time frame that is consistent with available resources.*
- Comment: The Commerce Department has already done this in its fiscal year 2002 and 2003 budget requests. The time frame for commodity classifications is set by statute.
- Recommendation: *Direct the respective entities within their departments to assess the amount of resources needed to make jurisdiction recommendations and determinations within established time frames, then either reallocate resources as appropriate or seek changes to the established time frame that are consistent with available resources.*

See comment 19.

**Appendix I: Comments from the Department
of Commerce**

Comment: As noted above, the Commerce Department has already done so.

Recommendation: *Revise interagency guidance to incorporate any changes to the referral process and time frames for making decisions.*

Comment: This recommendation will be covered in addressing the first recommendation.

**Appendix I: Comments from the Department
of Commerce**

The following are GAO's comments on the Department of Commerce's letter dated September 9, 2002.

GAO Comments

1. Commerce misrepresented our findings and conclusions because it incorrectly combined two different findings related to the commodity classification process by suggesting that we concluded that all 253 requests resulted in improper classifications. The 253 requests identified in our report represent cases that appear to meet the National Security Council or Commerce's stated referral criteria but were not referred to State and Defense for interagency review. Separately, our report discusses several instances in which Commerce improperly classified State-controlled items. We concluded that not referring commodity classification requests that appear to meet the referral criteria increases the risk of improper classification.

As already noted in our report, 212 commodity classification requests were returned to companies without classifications because Commerce determined that the items involved were either State-controlled or possibly State-controlled. Commerce's footnote acknowledges that these requests clearly meet the National Security Council referral criteria as they involve items "specifically designed, developed, configured, adapted, or modified for a military application," yet Commerce stated that it is not necessary to refer such requests. However, as stated in our report, we identified instances in which Commerce referred similar requests to State and Defense. We also found that by not consistently referring such requests, Commerce does not provide State with an opportunity to ensure that companies comply with the Arms Export Control Act. For example, we identified several companies that did not register with State after Commerce returned their classification requests and advised them that their items were State-controlled.

The identification of the remaining 41 classification requests that were not referred, despite appearing to meet the referral criteria, was based on our analysis of Commerce's data. We did not find any duplicates and were not able to independently verify Commerce's statement. We, therefore, have no basis for revising the numbers contained in our report.

2. Commerce maintains that an item appearing on both control lists does not necessarily mean that it is unclear which department has jurisdiction over the item, because Commerce's control list contains

**Appendix I: Comments from the Department
of Commerce**

technical control parameters that differentiate jurisdiction. We do not agree because Commerce's control list does not always provide such technical control parameters. For example, the requests we identified as having unclear jurisdiction were classified in Commerce Control List categories that either contain technical control parameters identical to those on the U.S. Munitions List or do not contain specific parameters to clearly differentiate those items that are Commerce-controlled.

3. As discussed in comment 1, these cases were identified as appearing to meet the referral criteria but were not referred to State and Defense.
4. We disagree that Commerce refers requests as required by the National Security Council guidance. As noted in our report, Commerce officials admitted that they inconsistently apply the guidance. Defense and State officials informed us that under their interpretations of the guidance, Commerce should be referring most, if not all, commodity classifications. The guidance does not provide a common definition of terms to be used when applying the criteria. Commerce officials informed us that they have never met with Defense or State officials to define key terms or to agree on a common interpretation of the guidance. Further, we disagree with Commerce's assertion that the 253 commodity classification requests that we identified represent all the requests that should have been referred. After reviewing a subset of Commerce data, we found at least 253 requests that appear to meet the referral criteria, but we did not conclude that this represents all the requests that should have been referred.
5. As discussed in our report, the departments have different interpretations of the National Security Council guidance, particularly as it relates to items derived from military applications. There is no "traditional" interpretation of the guidance. The example Commerce provides in its comments does not reflect the complexity or sensitivity of the types of items, such as night vision devices, which may meet the referral criteria.
6. The objectives of our report were to assess how Commerce and State, respectively, implement the commodity classification and commodity jurisdiction processes, not to assess the implementation of the National Security Council guidance as it relates to other processes such as licensing.

**Appendix I: Comments from the Department
of Commerce**

7. We assessed the implementation of the commodity jurisdiction process and did not evaluate the resulting determinations. In its implementation of the commodity jurisdiction process, State provides Commerce and Defense the opportunity to provide input on jurisdiction determinations and to escalate requests when there is a disagreement over the appropriate jurisdiction for an item.
8. Our report clearly reflects the nature of commodity classifications and the fact that they are not licensing determinations. We would note, however, that of the classifications provided by Commerce during our review period, about two-thirds involved classifications for items that generally would not require export licenses to most destinations. As a result, the classification process may be the only opportunity for State and Defense to become aware of what companies are exporting. While Commerce officials may be knowledgeable about the Commerce Control List, State and Defense officials have the authority and expertise to determine whether an item is covered by the U.S. Munitions List. The National Security Council guidance was issued to improve interagency coordination and transparency by providing State and Defense a role in the commodity classification process.
9. Our analysis of Commerce's median processing time for commodity jurisdiction cases is based on data provided by State. The median processing time, as contained in the report, reflects the amount of time that lapsed between when State referred the case to Commerce and when Commerce provided its initial input. Therefore, our calculation does not need to be revised.
10. See comments 1 and 15.
11. While Commerce notes that State and Defense have roles in reviewing Commerce's regulations and license applications, we are not incorporating this comment because it is not relevant to understanding the roles of these departments in the commodity classification process.
12. The technical data that Commerce refers to in its comment involved State-controlled missile technology that was exported to China based on an improper Commerce classification. A congressional inquiry determined that U.S. national security was harmed as a result. This incident highlights the risk of Commerce making commodity classification decisions without input from State and Defense. We note

Appendix I: Comments from the Department
of Commerce

that Commerce admits that jurisdiction is not always clearly delineated between Commerce and State regulations.

13. Our report identifies several instances in which Commerce improperly classified State-controlled items. The one case referred to in Commerce's comments involved explosive detection devices that were classified by Commerce but were later determined to be State-controlled through the commodity jurisdiction process. When these devices were reviewed through the commodity jurisdiction process, Commerce provided its recommendation on the appropriate jurisdiction and chose not to escalate State's determination that the items were State-controlled. As we explained to Commerce officials, we were unable to provide Commerce with documents or other evidence related to this case due to our policy to protect proprietary information.
14. As noted in comment 8, the National Security Council guidance provides a role for State and Defense in the commodity classification process. Furthermore, Commerce's comment reflects a disagreement with State and Defense as to which commodity classification requests should be referred in accordance with the guidance.
15. In our report, we identified three instances in which jurisdictional questions were raised during the license application review process. These license applications involved items for which Commerce had previously issued commodity classifications, but were identified by Defense in the license review process as being State-controlled. While Commerce may not agree with Defense's position, Commerce does not have the authority to determine which items are not subject to State's jurisdiction. By law, Commerce can only control, and therefore classify, items that are not controlled by another department. In its comments, Commerce refers to an interagency memorandum of understanding regarding which department has jurisdiction over certain night vision devices. However, there is currently an interagency disagreement on how the memorandum should be interpreted and, as mentioned in our report, an interagency debate on how night vision devices are to be controlled. Commerce also refers to the case involving the explosive detection devices and suggests that it did not improperly classify the devices. However, the devices were ultimately determined to be State-controlled through the commodity jurisdiction process, as discussed in comment 13. Also, we did not provide Commerce with the requested information because it was proprietary information obtained from other sources. While we did not discuss

**Appendix I: Comments from the Department
of Commerce**

these specific cases with Commerce officials to protect the identity of the companies involved, we did review government documents related to the cases and discussed the cases with company and other government officials.

16. Commerce states that when it returns a classification request to a company indicating that the item is subject to State's jurisdiction, it puts the company on notice. However, Commerce's practice does not provide State with an opportunity to obtain information on companies that need to register with State.
17. Our conclusion considers the effects our findings have on the entire export control system, which consists of separate regulatory regimes for defense and dual-use items. As noted in comments above, we did not attempt to identify all commodity classification requests that appear to meet referral criteria or those that resulted in improper classifications. The examples contained in the report are illustrative of weaknesses in Commerce's implementation of the commodity classification process. Furthermore, one improper classification can have serious implications for U.S. national security, as demonstrated by the release of missile technology to China discussed in the report. In discussing the impact on industry, Commerce's comments do not acknowledge that improper classifications can place companies at a competitive disadvantage. Specifically, a company may be exporting through State while its competitor may be exporting the same item through Commerce, based on an improper classification from Commerce.
18. The findings contained in our draft report were discussed in detail with Commerce officials before the draft was provided to Commerce for official comment. After considering Commerce's written comments, we are confident that the report accurately reflects information provided by Commerce, Defense, State, and company officials during our review.
19. We have revised our recommendation because Commerce believes that it cannot change the time frame for responding to commodity classification requests.

Appendix II: Comments from the Department of State

Note: GAO comments supplementing those in the report text appear at the end of this appendix.



United States Department of State

Washington, D.C. 20520

SEP 10 2002


Dear Ms. Westin:

We appreciate the opportunity to review your draft report, "EXPORT CONTROL: Processes for Determining Proper Control of Defense-Related Items Need Improvement," GAO-02-996, GAO Job Code 120062.

The Department's comments are enclosed for incorporation, along with this letter, as an appendix to the GAO final report.

If you have any questions regarding this response, please contact Peter Berry, Office of Defense Trade Controls, Bureau of Political Military Affairs on (202) 663-2806.

Sincerely,


Christopher B. Burnham
Assistant Secretary and
Chief Financial Officer

Enclosure:

As stated.

cc: GAO/ASM - Ms. Schinasi
State/OIG - Mr. Berman
State/PM - Mr. Maggi

Ms. Susan S. Westin,
Managing Director,
International Affairs and Trade,
U.S. General Accounting Office.

**Appendix II: Comments from the Department
of State**

Department of State Comments on GAO Draft Report

**EXPORT CONTROLS: Processes for Determining Proper Control
of Defense-Related Items Need Improvement**
(GAO-02-996, GAO Code 120062)

State Department comments on this draft report are set forth in detail. As always, Department officers are prepared to discuss and elaborate on these comments in person at any time.

The State Department welcomes the opportunity to comment on the draft report, entitled "Processes for Determining Proper Control of Defense-Related Items Need Improvement." We agree with your observation that what is controlled is fundamental to proper implementation of the system and we are committed to meeting established time lines. Over the past year have take steps to better do so. We appreciated the finding that the commodity jurisdiction ("CJ") requests managed by the Department were consistently transparent and coordinated interagency with Defense and Commerce in all instances. It would appear appropriate to highlight this more visibly in the draft report because the specific purpose of the April 15, 1996, NSC procedures on commodity jurisdiction and commodity classification is, as stated in that document, "to improve interagency coordination and transparency."

Your report recommended that the Department consider either assigning additional resources to the Office of Defense Trade Controls in order to meet the goal established in the NSC procedures of a 95-day cumulative timeline for responding to commodity jurisdiction requests submitted by exporters or revising the goal. We agree with the spirit of this objective and in March 2001, in response to a recommendation from the Department of State's Office of Inspector General, Office of Audits, did, in fact, assign an additional full time officer to the CJ function. Since then, there has been steady progress made in reducing timelines, as reflected in the following data (which we shared with the GAO team):

Table 1: Progress Toward 95-Day Cumulative Timeline

	<u>STATE/DTC</u>	<u>DOD/DTSA</u>	<u>DOC/BIS</u>
10/01/00-09/30/01	148 days	87 days	98 days

See comment 1.

See comment 2.

**Appendix II: Comments from the Department
of State**

03/12/01-07/30/02	133 days	86 days	88 days
10/01/01-07/31/02	113 days ¹	83 days	79 days

See comment 3.

The Department believes that at the current rate, the median overall timeline for CJs will be consistent with the NSC goal of 95 days by the end of the first half of fiscal year 03. If it is not, the Department will consider whether additional resources should be assigned or the timeline revised at that time. We are also instituting other enhancements consistent with our commitments to State's OIG. For example, we have entered into discussions with Commerce (BIS) to map-out a pilot program for full electronic CJ submissions. This program should be initiated during 2003. Similarly, as noted to the GAO audit team, we are developing an approach for making greater information available as a matter of public record on CJ determinations via the DTC Internet web site, while protecting those business interests accorded confidentiality under Section 38(e) of the AECA. This approach will also be initiated during 2003, subject to further consultation with the Department's Office of the Legal Adviser and with the U.S. defense industry through the relevant advisory committee (i.e., Defense Trade Advisory Group).

See comment 4.

Your report also recommended that "the Secretary of State direct the Office of Defense Trade Controls to issue initial determinations in accordance with the guidance" (even when other departments have not provided their input). We disagree with this recommendation in view of the overall improvement in CJ timelines (noted above) and in light of the longstanding policy and practice of ODTC, which the Department believes should continue, to accord great deference in this area to the national security views of the Department of Defense. A better approach, which we are following, is to enlist greater cooperation from other departments in meeting established timelines consistent with U.S. foreign policy and security interests. The Bureau of Political-Military Affairs is committed to adhering to established time lines and is approaching senior DoD officials to emphasize the importance of timely responses in CJ decision-making, and will also continue to

¹ 113 days represents the total median time required for all CJ processing in FY 2002 to date. For example, the 83 day median review time at DoD is included within the 113 days.

Appendix II: Comments from the Department of State

See comment 5.

remind other interagency participants of the established guidelines. If our approach does not produce the desired results over the next twelve months, we will re-examine your recommendations.

Related to your recommendations in this area, please allow us to point out also that the draft report appears to omit that ODTC is consistently meeting the 5-day timelines for initial referral of CJ applications to other agencies and that these referrals are for the express purpose (spelled-out in the NSC Procedures) of providing other departments with a basis upon which to submit recommendations to ODTC, preparatory to ODTC's initial determination. In this respect, it is not the case, as the draft report may unintentionally imply, that CJ submissions are not being acted upon until after the notional 55-day period for initial determination. The data on this point indicate that ODTC has consistently acted upon all CJ requests received from US exporters in a timely fashion:

Table 2: Referrals by State Now Beat 5-Day Initial Timeline

Interagency Referral by DTC	
10/01/97-09/30/01	6 Days
03/12/01-Present	4 Days

**Appendix II: Comments from the Department
of State**

The following are GAO's comments on the Department of State's letter dated September 10, 2002.

GAO Comments

1. While State consistently referred commodity jurisdiction requests to Commerce and Defense, we found indications in State's data that a limited number of requests were not referred to both departments. However, we could not confirm with State whether these cases were not referred because State officials did not provide responses to questions regarding specific jurisdiction requests.
2. During our review, State officials showed us the information contained in State's table 1. However, they did not provide us with the supporting data that would be needed to verify State's progress in reducing the amount of time to process jurisdiction requests. Furthermore, as noted in the report, State officials did not provide us with complete data for fiscal year 2001, despite our requests.
3. While we recognize State's efforts to reduce the amount of time to process jurisdiction requests, we note that the National Security Council guidance establishes 95 days as the maximum amount of time in which escalated cases are to be resolved. According to the guidance, final jurisdiction determinations should be issued in less than 65 days after a request is received, unless the case is escalated.
4. The issuance of an initial determination prior to receiving input from Defense or Commerce still provides Defense and Commerce an opportunity to express their views on the appropriate jurisdiction for an item, as those departments can escalate the initial determination if they disagree. Also, as discussed in the report, the issuance of an initial determination serves to increase the priority level Defense and Commerce assign to commodity jurisdiction reviews and is, therefore, a mechanism for facilitating the timely resolution of jurisdiction requests. We agree that State should emphasize to the other departments the importance of receiving timely input.
5. We revised the text to reflect the amount of time taken by State to refer jurisdiction requests to Defense and Commerce once it received the requests. Our analysis of State's data indicates that State took a median of 5 days to refer a request to Defense and 6 days to refer a request to Commerce for our review period.

Appendix III: Comments from the Department of Defense

Note: A GAO comment supplementing those in the report text appears at the end of this appendix.



OFFICE OF THE UNDER SECRETARY OF DEFENSE
2000 DEFENSE PENTAGON
WASHINGTON, DC 20301-2000

SEP 3 2002

I-02/011713

Ms. Katherine Schinasi
Director, Acquisition and Sourcing Management
U.S. General Accounting Office
441 G Street, N.W.
Washington, D.C. 20548

Dear Ms. Schinasi:

This is the Department of Defense (DoD) response to the GAO draft report, "EXPORT CONTROLS: Processes for Determining Proper Control of Defense-Related Items Need Improvement," dated August 8, 2002 (GAO Code 120062/GAO-02-996)."

Specific remarks related to your recommendations are attached. Thank you for the opportunity to comment on this draft report.

Sincerely yours,

Lisa Bronson
Deputy Under Secretary of Defense,
Technology Security Policy and
Counterproliferation

Attachment:
As stated



Appendix III: Comments from the Department
of Defense

GAO DRAFT REPORT – DATED AUGUST 8, 2002
GAO CODE 120062/GAO-02-996

“EXPORT CONTROLS: Processes for Determining Proper Control of
Defense-Related Items Need Improvement”

COMMENTS
TO THE RECOMMENDATIONS

RECOMMENDATION 1: To increase transparency to stakeholders and minimize the risk of Commerce making jurisdictional determinations through the commodity classification process, the GAO recommended that the Secretary of Commerce direct the Bureau of Industry and Security to promptly review existing guidance and develop, with the concurrence of the appropriate entities within State and Defense, criteria for referring commodity classification requests to those departments. In developing the criteria, the departments should agree on a common definition of terms to be contained in the criteria. Until the departments develop and implement referral criteria, the risk of Commerce improperly classifying State-controlled items will continue to exist. (p. 19/GAO Draft Report)

See comment 1.

RESPONSE: In many respects the existing guidance is generally straightforward. The larger problem is the lack of sufficient information contained in commodity classification requests. We are prepared to work with Commerce to develop and implement additional referral criteria.

RECOMMENDATION 3: To insure that Commerce has sufficient information to make timely and appropriate commodity classifications, we recommend that the Secretary of Commerce direct the Bureau of Industry and Security to revise guidance for companies on the information to be provided with commodity classification requests and consider including a requirement for information on an item’s origins and applications.

RESPONSE: Although this recommendation is not directed to DoD, we concur with this recommendation, particularly regarding the inclusion of a requirement for information on an item’s origins and applications to be mandatory information submitted with commodity classification requests. Such information should not only improve the timeliness and quality of the Commerce response, but also reduce the number of classification requests referred to the commodity jurisdiction process due to insufficient information. We are prepared to assist Commerce in revising guidance related to commodity classification requests and suggest that this could be done in conjunction with the GAO’s recommended development and implementation of commodity classification referral criteria (see Recommendation 1).

**Appendix III: Comments from the Department
of Defense**

RECOMMENDATION 5: To improve the timeliness of the commodity jurisdiction process, the GAO recommended that the Secretaries of State, Commerce, and Defense direct the respective entities within their departments to assess the amount of resources needed to make jurisdiction recommendations and determinations within established time frames, then either reallocate resources as appropriate or seek changes to the established time frame that are consistent with available resources. (p. 19/GAO Draft Report)

RESPONSE: As noted in your report, DTSA has recently hired an additional staff person to work on commodity jurisdiction requests. While we anticipate that this action will greatly contribute to reducing Defense processing time, we will continue to monitor and assess the overall commodity jurisdiction review process and take further action as necessary.

RECOMMENDATION 6: To improve transparency and consistency of the commodity classification and jurisdiction processes, the GAO recommended that the Secretaries of State, Commerce, and Defense revise interagency guidance to incorporate any changes to the referral process and time frames for making decisions. (p. 20/GAO Draft Report)

RESPONSE: We are prepared to work with State and Commerce to improve transparency and consistency of both the commodity classification and commodity jurisdiction processes.

**Appendix III: Comments from the Department
of Defense**

The following is GAO's comment on the Department of Defense's letter dated September 3, 2002.

GAO Comment

1. Because Commerce, State, and Defense officials expressed different interpretations of the National Security Council guidance during our review, we do not agree that the existing guidance is generally straightforward.

Appendix IV: GAO Contact and Staff Acknowledgments

GAO Contact

Anne-Marie Lasowski, (202) 512-4146

Acknowledgments

John Neumann, Johana R. Ayers, Raymond H. Denmark, W. William Russell IV, Richard K. Geiger, Markques Y. McKnight, and Christina Sklarew also made significant contributions to this report.

Related GAO Products

Defense Trade: Lessons to Be Learned from the Country Export Exemption. [GAO-02-63](#). Washington, D.C.: March 29, 2002.

Export Controls: Reengineering Business Processes Can Improve Efficiency of State Department License Reviews. [GAO-02-203](#). Washington, D.C.: December 31, 2001.

Export Controls: Clarification of Jurisdiction for Missile Technology Items Needed. [GAO-02-120](#). Washington, D.C.: October 9, 2001.

Defense Trade: Information on U.S. Weapons Deliveries to the Middle East. [GAO-01-1078](#). Washington, D.C.: September 21, 2001.

Export Controls: State and Commerce Department License Review Times Are Similar. [GAO-01-528](#). Washington, D.C.: June 1, 2001.

Export Controls: Regulatory Change Needed to Comply with Missile Technology Licensing Requirements. [GAO-01-530](#). Washington, D.C.: May 31, 2001.

Defense Trade: Observations on Issues Concerning Offsets. [GAO-01-278T](#). Washington, D.C.: December 15, 2000.

Defense Trade: Data Collection and Coordination on Offsets. [GAO-01-83R](#). Washington, D.C.: October 26, 2000.

Defense Trade: Contractors Engage in Varied International Alliances. [GAO/NSIAD-00-213](#). Washington, D.C.: September 7, 2000.

Defense Trade: Analysis of Support for Recent Initiatives. [GAO/NSIAD-00-191](#). Washington, D.C.: August 31, 2000.

Foreign Military Sales: Changes Needed to Correct Weaknesses in End-Use Monitoring Program. [GAO/NSIAD-00-208](#). Washington, D.C.: August 24, 2000.

Defense Trade: Status of the Department of Defense's Initiative on Defense Cooperation. [GAO/NSIAD-00-190R](#). Washington, D.C.: July 19, 2000.

Defense Trade: Identifying Foreign Acquisitions Affecting National Security Can Be Improved. [GAO/NSIAD-00-144](#). Washington, D.C.: June 29, 2000.

Related GAO Products

Foreign Military Sales: Efforts to Improve Administration Hampered by Insufficient Information. [GAO/NSIAD-00-37](#). Washington, D.C.: November 22, 1999.

Foreign Military Sales: Review Process for Controlled Missile Technology Needs Improvement. [GAO/NSIAD-99-231](#). Washington, D.C.: September 29, 1999.

Defense Trade: Department of Defense Savings from Export Sales Are Difficult to Capture. [GAO/NSIAD-99-191](#). Washington, D.C.: September 17, 1999.

Defense Trade: Status of the Defense Export Loan Guarantee Program. [GAO/NSIAD-99-30](#). Washington, D.C.: December 21, 1998.

Defense Trade: U.S. Contractors Employ Diverse Activities to Meet Offset Obligations. [GAO/NSIAD-99-35](#). Washington, D.C.: December 18, 1998.

Defense Trade: Weaknesses Exist in DOD Foreign Subcontract Data. [GAO/NSIAD-99-8](#). Washington, D.C.: November 13, 1998.

GAO's Mission

The General Accounting Office, the investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through the Internet. GAO's Web site (www.gao.gov) contains abstracts and full-text files of current reports and testimony and an expanding archive of older products. The Web site features a search engine to help you locate documents using key words and phrases. You can print these documents in their entirety, including charts and other graphics.

Each day, GAO issues a list of newly released reports, testimony, and correspondence. GAO posts this list, known as "Today's Reports," on its Web site daily. The list contains links to the full-text document files. To have GAO e-mail this list to you every afternoon, go to www.gao.gov and select "Subscribe to daily E-mail alert for newly released products" under the GAO Reports heading.

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are \$2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. General Accounting Office
441 G Street NW, Room LM
Washington, D.C. 20548

To order by Phone: Voice: (202) 512-6000
 TDD: (202) 512-2537
 Fax: (202) 512-6061

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm

E-mail: fraudnet@gao.gov

Automated answering system: (800) 424-5454 or (202) 512-7470

Public Affairs

Jeff Nelligan, managing director, NelliganJ@gao.gov (202) 512-4800
U.S. General Accounting Office, 441 G Street NW, Room 7149
Washington, D.C. 20548

EXHIBIT 4

UNCLASSIFIED

**United States Department of State
and the Broadcasting Board of Governors**

Office of Inspector General

**Review of the U.S. Munitions
List and the Commodity
Jurisdiction Process**

Memorandum Report 01-FP-M-027, March 2001



IMPORTANT NOTICE

This report is intended solely for the official use of the Department of State or the Broadcasting Board of Governors, or any agency or organization receiving a copy directly from the Office of Inspector General. No secondary distribution may be made, in whole or in part, outside the Department of State or the Broadcasting Board of Governors, by them or by other agencies or organizations, without prior authorization by the Inspector General. Public availability of the document will be determined by the Inspector General under the U.S. Code, 5 U.S.C. 552. Improper disclosure of this report may result in criminal, civil, or administrative penalties.

UNCLASSIFIED

OFFICE OF INSPECTOR GENERAL
MEMORANDUM REPORT 01-FP-M-027
REVIEW OF THE U.S. MUNITIONS LIST AND THE COMMODITY
JURISDICTION PROCESS
MARCH 2001

EXECUTIVE SUMMARY

The National Defense Authorization Act for FY 2000, Public Law 106-65, Title XIV, Section 1402, Annual Report on Transfers of Militarily Sensitive Technology to Countries and Entities of Concern, requires the Inspectors General of the Departments of Commerce, Defense, Energy, and State to audit the U.S. Government policies and procedures for export of technologies and technical information to countries and entities of concern. The law specifies that these Inspectors General submit an annual report due March 31 of each year beginning in 2000 and ending in 2007. During FY 2001, the Department of State Office of Inspector General (OIG) assessed the export licensing process to determine whether the policies and procedures for developing, maintaining, and revising the U. S. Munitions List (USML) were adequately protecting the export of militarily sensitive technologies. As part of this objective, we also assessed the policies and procedures in place at the Office of Defense Trade Controls (DTC) for processing commodity jurisdiction cases in a timely and transparent manner. Through the commodity jurisdiction process, DTC advises exporters on whether an item is subject to the USML.

OIG found that the policies and procedures for developing, maintaining, and revising the USML were adequately protecting the export of militarily sensitive technologies. Our review of selected commodity jurisdiction cases indicated that the Department of State (the Department) consistently gave deference to the views of the national security agencies in making a commodity jurisdiction determination. Additionally, DTC concurred with recommendations made by a defense or intelligence agency. We found, however, that the policies and procedures for the commodity jurisdiction process needed improvement. The process took too long and was not always transparent. OIG also found that DTC had not performed a comprehensive review of the USML since 1993. OIG believes that Defense Trade Security Initiative (DTSI) number 17, which calls for a multiyear review of all USML categories, is a good way to revise and potentially improve the wording and descriptions of certain USML categories and commodities.

SCOPE OF REVIEW

The primary objective of this review was to evaluate the process for placing items on the USML and the policies and procedures for considering amendments and revisions to it. We also assessed the policies and procedures in place at DTC for processing commodity jurisdiction cases in a timely and transparent manner. In conducting this review, we interviewed Department officials and reviewed documents at DTC, including the International Traffic in Arms

Regulations (ITAR) and commodity jurisdiction files and records. In addition, we discussed the USML and the commodity jurisdiction process with exporters and a Washington, DC, think tank. We also spoke with officials from the Departments of Commerce, Defense, and Energy. The work was performed between October 2000 and January 2001. Major contributors to this report were Max Aguilar, Herbert Harvell, and Bryan Tenney.

BACKGROUND

The U.S. Munitions List

The United States controls the export of certain goods and technologies for national security, foreign policy, or nonproliferation reasons under the authority of several laws. The principal legislation for controlling the export of goods and technologies with military capabilities is the Arms Export Control Act of 1976. Under the Arms Export Control Act, the President has primary responsibility for designating items on the USML as defense articles or services. In Executive Order 11958, the President delegated this authority to the Secretary of State. Within the Department, the Bureau of Political-Military Affairs, DTC, licenses U.S. companies that export munitions commodities. Munitions commodities are items that only have military uses, such as long range missiles. DTC uses the ITAR to administer its authority under the Arms Export Control Act. The ITAR contains regulations that companies must follow to submit a license. The ITAR also contains the USML, which identifies those items, technologies, and services that have been specifically designed, developed, configured, adapted, or modified for a military application, and could, if exported, jeopardize national security or foreign policy interests of the United States. The USML has 21 categories.

The Commodity Jurisdiction Process

If an exporter is uncertain whether an article or service is covered by the USML, DTC provides a determination using commodity jurisdiction procedures. An exporter's commodity jurisdiction request identifies the product, article, or services in question and includes a history of the product's design. The determination process entails consulting among the Departments of Commerce, Defense, and State, and other government agencies and industry in appropriate cases. The Departments of Commerce and Defense provide the technical analysis on the request and send their recommendations to DTC. DTC then analyzes the recommendations and makes a decision on whether the commodity is a USML item. A DTC official stated that the commodity jurisdiction process was developed to help the exporter.

National Security Council Guidelines

In April 1996, the National Security Council (NSC) issued guidelines on how the State Department commodity jurisdiction and Commerce Department commodity classification processes are supposed to work. An NSC official stated that the 1996 guidance was the result of interagency coordination at the Assistant Secretary and Deputy Assistant Secretary levels at the Departments of Commerce, Defense, and State. The guidance was created because of a great

deal of disagreement between Commerce and State about the way commodity jurisdictions and classifications were being granted at those Departments.

The NSC commodity jurisdiction guidelines specify that a decision will be made within a 95-calendar-day cumulative timeline (starting from the date DTC receives a complete commodity jurisdiction request). The time is allocated as follows:

Routine Determination (up to 60 days)

- Referral by DTC of commodity jurisdiction applications to other agencies: 5 days
- Departments submit recommendations to Director of DTC
(Departments may request 10 additional days to submit
recommendations for extraordinary cases): 35 days
- Decision by Director of DTC: 10 days

First escalation period (up to 15 days)

- Escalation period for the Department(s) contesting the DTC decision: 5 days
- Decision by Department of State Assistant Secretary for Political-Military
Affairs: 10 days

Second escalation period (up to 15 days)

- Escalation period for the Department(s) contesting the Assistant
Secretary's decision: 5 days
- Decision by Department of State Under Secretary/Secretary: 10 days

Third escalation period (up to 5 days)

- Escalation period for the Department(s) contesting the Under Secretary's/
Secretary's decision: 5 days
- Right of escalation up to the President of the United States:

Previous Work

In June 1999, OIG issued a report entitled *Export Licensing* (99-CI-018). This audit found that, overall, the export licensing process is working as intended and that the Department consistently executed its export licensing responsibilities in accordance with established policies and procedures. However, OIG found that the end-use monitoring (Blue Lantern program)

process used in munitions licensing could be improved by: 1) placing more emphasis on the selection criteria used to initiate Blue Lantern checks, 2) closely monitoring the requests that overseas posts are tasked to complete, and 3) ensuring overseas posts have the technical expertise to conduct the checks. OIG also found that supervisory reviews of routine license processing and additional training opportunities for licensing officers was needed. OIG concluded that these needs were symptomatic of a larger problem at DTC – insufficient resources to meet its expanding mandate. Overall, OIG made 11 recommendations to DTC. DTC agreed with 9 of the 11 recommendations and took appropriate steps to comply with the 9. Of the 11 OIG recommendations, 7 are closed, and 4 require additional work to be closed.

In March 2000, OIG issued a report entitled *Department of State Controls Over the Transfer of Militarily Sensitive Technologies to Foreign Nationals from Countries and Entities of Concern* (00-CI-008). OIG found that DTC did not systematically track foreign nationals listed on export licenses, but instead relied heavily on self-policing by U.S. companies supplemented by a few selected compliance reviews. Therefore, although licensing agreements may have been in place requiring adherence to policies and procedures protecting sensitive information, the risk of unauthorized release persisted. OIG recommended that DTC improve the Department's ability to monitor the transfer of technical information to foreign nationals and inform responsible parties of applicable licensing requirements. Overall, OIG made three recommendations to DTC. DTC agreed with all three. Of the three recommendations, one is closed, and two require additional work to be closed.

RESULTS OF REVIEW

The U.S. Munitions List

OIG found that the policies and procedures for developing, maintaining, and revising the USML were adequately protecting the export of militarily sensitive technologies. However, DTC had not performed a comprehensive review of the USML since 1993. OIG believes that the DTSIs, especially number 17, which calls for a multiyear review of USML categories, are a good way to revise and potentially improve the wording and descriptions of certain USML categories and the commodities controlled on the USML.

USML Revisions

There are very few revisions to the USML. DTC officials stated that changes to the USML occur infrequently because of the nature of the commodities controlled. DTC cannot unilaterally recommend placing items on the USML because the office neither develops military sensitive technology, nor has the technical capacity to make such decisions. The Department of Defense research labs, for example, can recommend that a new technology be added to the USML. Congress and the President can also make changes to the USML. The most recent addition to the USML was made when Congress gave the satellite category back to the Department of State (from the Department of Commerce) in March 1999. All changes to the USML are reported in the *Federal Register* and the Department must submit a report to Congress at least 30 days before any item is removed from the USML.

During our review, we found that some in the export community believed that the U.S. Government is controlling too many commodities on the USML. For example, a major Washington, DC, think tank, the Center for Strategic and International Studies, conducted a study on the U.S. military export control system and summarized that:

The U.S. export control system for military equipment that has evolved over the past 40 years is viewed as increasingly counterproductive. Controls on military exports were designed to protect American technology and serve as a tool of foreign policy. The current architecture of export controls was developed in the 1970s, but business practices have evolved substantially since that time. Rather than protecting technology, the system now causes larger security problems. Export controls are driving a wedge between the United States and its allies and causing other countries to avoid American technology and components because of frustrations with the export licensing process. Interoperability between U.S. and allied forces in the field will suffer.

Part of the frustration expressed by the Center for Strategic and International Studies stems from the fact that the USML is not examined periodically to ensure that it is still meeting its objectives under the Arms Export Control Act. DTC did not have a mechanism for periodic reviews of the USML and for determining whether commodities currently controlled still merited being on the USML. DTC officials last performed a comprehensive “scrub” of the USML at the beginning of 1993 at the directive of the President. Department of Defense officials were consulted, and the results of the review were reported in a *Federal Register* notice dated July 22, 1993. The DTC official that worked on the 1993 review indicated that a few categories in the USML could still be revised to clarify wording and commodity descriptions.

A September 1999 Department of Defense White Paper on Arms and Technology Transfer concluded, “The USML should be reviewed to identify items and technologies that should no longer be controlled either because they represent low-risk transactions, or because of their widespread availability, are no longer controllable.” Because no entity has done a comprehensive analysis of all USML categories in approximately 8 years to determine whether the commodities controlled on it are in accord with current day realities, a detailed, thorough review of the list is needed. As this report was being written, the Department of Defense, under DTSI 17, was undertaking just such a review.

Defense Trade Security Initiative Number 17

In May 2000, a series of DTSIs were announced by the Secretary of State. The objective of those initiatives is to improve export controls. One initiative, number 17, calls for a periodic review of the USML. In response to DTSI 17, Defense drafted a plan for reviews of approximately one-quarter of the USML per year. The plan lists four goals of the reviews: identification of USML items that are more properly controlled on the Commerce Control List (CCL); identification of items that should no longer be controlled on either the USML or the CCL; identification of additions to the USML, primarily because of new technological developments; and clarification of USML language to ensure that users of the list can easily

identify the items requiring export licenses. The five USML categories that are currently under review by the Department of Defense are firearms, explosives, aircraft, toxicological agents, and nuclear weapons. After Defense develops its specific recommendations pertaining to the USML, it will consult with DTC about the findings. The director of DTC agreed that the USML should be reviewed periodically. However, he stated that it would only be useful if the review updated and clarified relevant categories, but not if it were used merely to accomplish the objective of “dumbing down” the USML to make it better resemble the CCL through removal of military parts and components from the USML to the benefit of the international gray arms market and other criminal elements.

The Department of Defense White paper, the findings of the Center for Strategic and International Studies, and the DTSI, illustrate that there is a strong body of thought that reviewing the USML periodically is beneficial. OIG believes that the planned review of the USML is a good plan of action. If commodities controlled on the USML no longer present national security or foreign policy dangers, then the items should be removed from the list. Therefore, we concluded that DTSI 17 is needed and the cycle of USML category reviews begun in May 2000 should be continued into the future.

Commodity Jurisdiction Process

Annually, DTC receives 200-400 commodity jurisdiction requests. During the course of our review, we audited the FY 2000 commodity jurisdiction cases processed at DTC. In FY 2000, DTC received 220 commodity jurisdiction requests. As of November 2000, of the 220 requests, DTC had issued jurisdictional rulings for only 103 of those items; 117 items were still awaiting a determination by DTC. Of the 103 jurisdictional rulings, 56 were determined to be CCL jurisdictional items, 29 were USML jurisdictional items, 7 were split jurisdictions (both CCL and USML), 8 were returned without action for lack of information, and 3 were withdrawn by the exporter. OIG selected a judgmental sample of 20 commodity jurisdiction cases from the 103 jurisdictional rulings for FY 2000.

The sample of 20 cases OIG examined included the following:

- all 7 cases where split jurisdiction was recommended by DTC,
- 6 cases where DTC ruled USML jurisdiction after receiving conflicting recommendations from Defense and Commerce,
- 2 cases where the jurisdictional request had not been referred to Defense and Commerce, and
- 5 randomly selected cases from the remaining 88 rulings that had been completed by DTC in FY 2000.

Based on reviewing the files for the sample cases, we found that the policies and procedures for the commodity jurisdiction process were adequate; however, two components of

the process need improvement. OIG found that the process took far too long and was not always transparent.

Timeliness of the Commodity Jurisdiction Process Needs Improvement

As highlighted in the background section of this report, routine commodity determination should take no more than 60 calendar days. The commodity jurisdiction process at DTC, however, took an excessive amount of time. The average processing time for the 20 cases in our sample was 196 calendar days, or almost 6 1/2 months. However, in two cases, the request was not properly referred out per the NSC guidelines, which significantly decreased the amount of time to grant a determination. If these cases are not included in the calculation, the average processing time increases to 214 days, or a little over 7 months. Also, in one case, a company was applying for small technical modifications to a prior determination and not an actual commodity jurisdiction ruling. This case was only referred to Defense. Because the company was not asking for reconsideration on the jurisdiction, Defense replied in only 19 calendar days and the answer was sent out by DTC in 35 calendar days. If this case is also taken out of the calculation, the average increases to 224 calendar days, or 7 1/2 months. This amount of processing time is far too long, especially taking into account that many of the exporters making the requests work in fast-paced environments where decisions have to be made quickly. OIG believes that DTC should make every effort to process the cases within the NSC 60-day guidance.

There are two reasons why the commodity jurisdiction process took so long at DTC. First, the Departments of Commerce and Defense have been extremely slow to respond to DTC's referrals. In one case in our sample, it took Commerce 289 calendar days to respond to DTC. In other cases in our sample, it took Commerce 180, 163, and 155 calendar days to respond. Also, in all FY 2000 commodity jurisdiction requests DTC received, there were several other cases (not in our sample) that were at Defense and Commerce for more than 200 calendar days, and 95 cases as those agencies for than 100 days. Overall, in the 20 cases in the FY 2000 sample, Commerce averaged 110 calendar days to respond to commodity jurisdiction requests, and Defense averaged 88 calendar days to respond. For all FY 2000 cases closed at DTC, Defense averaged 76 calendar days to respond, and Commerce averaged 117 calendar days. Using the NSC guidelines, Commerce and Defense should return their recommendations to DTC in 35 days, except in an extraordinary case. In that case, the agencies are granted another 10 days.

DTC did not impose or enforce deadlines on Commerce or Defense. OIG believes that a DTC notification process of sending letters to Commerce and Defense when a deadline is approaching and when a deadline has passed would help ensure that Commerce and Defense get their recommendations to DTC within the NSC time guidelines and, as a byproduct, improve responsiveness to exporters.

Recommendation 1: We recommend that the Office of Defense Trade Controls develop procedures to regularly notify the Departments of Commerce and Defense of deadlines for specific cases, in order to conform with the National Security Council time guidelines.

DTC agreed with this recommendation and will enforce systematic deadlines on the other agencies.

The second reason for the long processing time of commodity jurisdiction requests at DTC is because even in the cases where Defense and Commerce responded in a relatively timely fashion, in many instances, DTC still took months to issue a determination. For example, in one case, it took the exporter 10 months to get an answer from DTC, even though Commerce and Defense returned their recommendations to DTC within 3 1/2 months. In another case, it took an exporter almost 11 months to get a response from DTC, although DTC had received the Commerce and Defense recommendations within 3 1/2 months. DTC officials stated that this case involved interagency dispute, and a meeting was held with the company, at their request, prior to DTC's issuance of the final letter. The slow processing time at DTC contradicts the NSC guidance, which states that the process is supposed to take no more than 60 calendar days from start to finish. In our sample, we found that commodity jurisdiction cases took an average of 195 calendar days. This abnormally long processing time does not present the general public with a positive image of dealing with the U.S. Government.

Recommendation 2: In coordination with recommendation 1, we recommend that the Office of Defense Trade Controls develop and implement a plan to improve its commodity jurisdiction procedures in order to meet the National Security Council time guidelines.

DTC agreed with this recommendation and will try to improve its own deadlines. DTC plans to deploy additional resources to accomplish this.

DTC officials provided several explanations on why it took so long to process commodity jurisdiction requests. First, DTC cited a continuing staffing problem. As a result, for up to 6 months during FY 2000, an officer at DTC was not assigned to cover the commodity jurisdiction process. During this time, the commodity jurisdiction portfolio was given to a manager who was already heavily burdened and did not give his full attention to the commodity jurisdiction process. Second, a DTC official stated that the office has higher priorities than the commodity jurisdiction process; its highest priority is to process approximately 44,000 export licenses annually. Third, DTC officials believe that some exporters have distorted the intent of the commodity jurisdiction process, which was originally supposed to be a vehicle to help the exporter. Because some companies submit the same request multiple times without submitting new data, DTC officials believe that, in some cases, the process has evolved beyond its original intent and that some exporters are attempting to get DTC to take their particular commodity off the USML. Last, a DTC official stated that in some cases the delays were due to the type of commodities and their complexity.

In OIG's 1999 audit report on export licensing, we found that inadequate resources had made it increasingly difficult for DTC to meet its broadening mandate. During discussions with the director of DTC for this review, OIG learned that the resource authorization situation has been alleviated, due to an early decision by Secretary Powell to approve recruitment and full staffing of DTC at authorized full-time equivalent (FTE) levels and expedited security

clearances. As of March 11, 2001, DTC has 71 FTE authorized and 55 full-time State employees on board. The office has also enlarged its staff of military officers on detail from the Pentagon from four to eight, drawing on funds made available by Congress in the FY 1999 National Defense Authorization Act. In order to provide an appropriate career path and be consistent with “notwithstanding” provisions related to grade structure enacted in the Foreign Relations Authorization Act for FY 2000 and 2001, six new GS-14 positions and three new GS-15 positions have been established within the authorized personnel ceiling. Full staffing is expected by the Summer of 2001. OIG believes that when DTC staffing initiatives have been completed, this should help it accomplish its mandated workload within NSC guidelines.

Better Transparency is Needed in the Commodity Jurisdiction Process

The ITAR requires that all commodity jurisdiction cases be sent to Commerce and Defense. DTC, however, was not referring all commodity jurisdiction requests to Commerce and Defense, thus calling into question the transparency of the process. In our sample, there were two cases that were not staffed out to Commerce and Defense. In the first case, a DTC official stated that it was obvious that the commodity (F-16 Aircraft Hydraulic Speed Brake Values) was a USML item, so DTC did not go through the formal procedures of asking Commerce and Defense for their recommendations. DTC did send Commerce a fax informing it of what it had done with the case. Commerce then sent a fax back agreeing with DTC’s action. Overall, DTC processed this case in just 7 calendar days. In the second case, the item was also obviously a USML item (Technical Drawings and Blueprints Created for the U.S. Air Force Entitled: “BLU-109/B Bomb, 2000 lb., Penetrator Explosive;” Created by Lockheed Missiles & Space Company, Inc;). Therefore, DTC did not refer it out, although it did fax Commerce and Defense its intentions – Defense concurred, and Commerce did not contest it.

As stated above, the ITAR states that DTC shall notify Commerce and Defense of the initiation of each case. When cases are not referred to Commerce and Defense, those agencies have no way to recommend whether the commodity is a USML or a CCL item. It also sheds doubt upon why DTC was not referring all cases to Commerce and Defense. Consequently, in the future, all commodity jurisdiction cases should be properly referred to Commerce and Defense, both the initiation and the resolution of the case.

Recommendation 3: We recommend that the Office of Defense Trade Controls inform the relevant agencies of all the commodity jurisdiction requests it receives and inform relevant agencies of its decision on each jurisdiction request.

DTC disagreed with the recommendation. DTC believes that the premise of OIG’s recommendation is that the relevant agencies are not being informed of all commodity jurisdiction requests and all decisions taken on them. They stated that the crux of OIG’s recommendation relates to two cases where, in fact, the agencies were informed of both requests and both decisions, but after DTC made an initial ruling. They also stated that OIG cites two cases out of hundreds available to it.

OIG disagrees with DTC's response on two counts. First, there were not "hundreds" of cases, because DTC only processed 103 of 220 cases they received in FY 2000. Of that 103, OIG sampled 20, where we found 2 cases (10 percent) that were not properly referred to the other agencies according to both the ITAR and the NSC guidelines. Second, despite the fact that OIG recognized that these were "obviously" USML items, DTC still did not follow the ITAR and NSC guidelines, which clearly state that DTC shall notify Commerce and Defense of the initiation of each case.

Another transparency-related issue in the commodity jurisdiction process is that Commerce and Defense were unable to see each other's positions on a case unless they specifically asked for it. Consequently, Commerce and Defense did not know whom the other agency recommended as the jurisdictional authority. The system also relied on both Commerce and Defense sending couriers to pick up each individual commodity jurisdiction package, and signed and dated commodity jurisdiction letters. Each commodity jurisdiction package contains background information submitted by the exporter on the particular commodity. This arrangement has also resulted in problems because, according to the DTC commodity jurisdiction officer, occasionally Commerce claimed a specific commodity jurisdiction case was not included in a package months after it was picked up.

DTC did not have a computer interface with the other agencies involved in the commodity jurisdiction process. DTC did not even have an external, unclassified e-mail system. Therefore, if agencies had questions pertaining to the status of a specific case, they had to call DTC. Also, because no computer interface existed for commodity jurisdiction cases, history on specific types of commodities was unavailable to Commerce or Defense. A computer database providing historical knowledge to all agencies involved in this process would be useful for several reasons. First, it could be helpful in reviewing commodity jurisdiction resubmissions from the same company or for like products. Second, it would be favorable if the situation arises again where DTC does not have an officer covering the commodity jurisdiction process full-time. The person temporarily covering the process could access the database and obtain historical data on the particular commodity. Third, a computer database could also improve timeliness by electronically warning Commerce and Defense when they are approaching a deadline.

Overall, OIG believes that automation of the commodity jurisdiction process would be an excellent method to improve interagency communication and solve the problems related to timeliness and transparency noted above. OIG believes that a secure system interface between the Departments of Commerce, Defense, and State is technologically feasible. Relying on manual, paper processes in the modern day world is outdated. Because there is no system interfaces between the agencies involved in the commodity jurisdiction process, the process is inhibited from running as smoothly as it could. Improved transparency and timeliness in the commodity jurisdiction process could be achieved through automation of the process, whether through the use of a database accessible by Commerce and Defense, or at the least, e-mail connectivity.

Recommendation 4: We recommend that the Office of Defense Trade Controls create a more efficient and transparent commodity jurisdiction process by coordinating with the Departments of Commerce and Defense to obtain a secure automated system for processing, referring, and storing historical data on commodity jurisdiction cases.

Recommendation 5: We recommend that the Office of Defense Trade Controls coordinate with the Bureau of Information Resource Management and establish an e-mail system.

DTC requested that the consideration of these recommendations be deferred until the next congressionally mandated audit, which will examine the information technology systems at each of the agencies involved in the export licensing process and their compatibility. This audit is scheduled to begin in the spring of 2001.

Because the next joint-OIG audit will examine the information technology systems at each of the agencies involved in the export licensing process and their compatibility, OIG agrees to defer these issues until the next report, with the caveat that these recommendations be fully examined and potentially implemented then.

Unresolved Jurisdiction Issues Concerning Night-Vision Technology

Night-vision technology-related commodities are an example of where the USML and CCL must be clarified. Since 1998, Commerce and State have disputed which agency has jurisdictional authority for certain night-vision technologies. In 1992, a classified memorandum of understanding (MOU) was signed between the Departments of Commerce, Defense, and State concerning night-vision technology. A Department of State official in the Bureau of Nonproliferation (NP) indicated that the MOU worked fine until 1998. Then, however, controversy ensued because the MOU was ignored, partially due to rapid changes in night-vision technology. It became unclear where certain night-vision commodities should be licensed, at DTC under the USML or at Commerce under the CCL. The NP official explained that the controversy was exacerbated because Defense began sending recommendations on night-vision commodities to Commerce that sometimes recommended USML and sometimes did not. Concurrently, the political pendulum started to shift toward procontrol views with the report by the Cox Committee. Simultaneously, a case pertaining to one of the disputed night-vision commodities had been escalated to the NSC by Commerce. The NSC, however, has not yet ruled on the case.

OIG was informed that a dialogue started in the fall of 1999 related to the night-vision commodities in dispute. Attempts to resolve the controversy failed and the dispute continued to fester among the agencies. According to an NP official, it was evident that there were enormous problems defining a system versus a component related to certain night-vision technologies, and Defense was unwilling to decide whether these commodities were CCL or USML. An interagency meeting hosted by Defense convened in April 2000. Defense, five industry representatives, Commerce, and a State Department NP official attended the meeting. DTC was invited, but was unable to attend. The meeting's goal was to come to some consensus on the

night-vision commodities in dispute. However, even after the meeting, the NP official felt that the controversy was not resolved. The NP official commented in November 2000:

The exporter is in real limbo. This has been a 15-to-16-month process. A policy of comity on these commodities has been suspended. We are killing the manufacturers of sensor equipment (a night-vision technology) because of arbitrariness. The overwhelming impression is that we are doing this to the export community because we can. We have to have a real determination on some of these things (as to whether they are USML or CCL).

The dispute over which agency, the Department of Commerce or the Department of State or both, should have jurisdiction over night-vision commodities must be resolved. If the Commerce, Defense, and State Departments renegotiated the 1992 night-vision commodities MOU, it could provide the framework for delineating future commodity, system, and component licensing procedures. Additionally, OIG believes that the DTSI 17 process for 2002 could provide a review of the USML category that covers night-vision technology and aid interagency cooperation on this intricate commodity.

Recommendation 6: We recommend that the Office of Defense Trade Controls coordinate with the Departments of Commerce and Defense in updating the 1992 memorandum of understanding on night-vision commodities and request that the Department of Defense add the U.S. Munitions List category for night-vision commodities to the DTSI Number 17 review for 2002.

DTC disagrees with this recommendation. They stated that responsibility for renegotiating the MOU resides with the Department's Bureau of Nonproliferation, Office of Export Controls and Conventional Arms Nonproliferation Policy. Concerning the second part of the recommendation, DTC proposed that night-vision technologies and space-qualified items be part of the first year review by Defense under DTSI 17. Because their proposal was not agreed upon, DTC has already initiated the process to bring about resolutions to the current cases identified by OIG.

OIG's recommendation is that the agencies involved in this dispute resolve the problem. OIG will close this recommendation when DTC, as the Department's jurisdiction authority, in coordination with the Departments of Defense and Commerce, has resolved the issue.

No Written Guide for the Government Jurisdiction Process

Because of the interagency impasse on the night-vision commodities, the Office of Export Control and Conventional Arms Nonproliferation Policy initiated the government jurisdiction process. The government jurisdiction process is supposed to work in a manner similar to DTC's commodity jurisdiction process, except in this case, it is a government agency that is initiating the request, rather than an exporter. OIG notes that DTC is in charge of the government jurisdiction process and opened 14 government jurisdiction requests in FY 2000. Of the 14 requests, DTC issued two rulings. Out of the 14 government jurisdiction cases opened by

DTC in FY 2000, 6 were initiated by the Department of Defense, 7 by the U.S. Customs Service, and 1 by the Department of Energy.

To resolve the night-vision technology deadlock, the Office of Export Control and Conventional Arms Nonproliferation Policy sent a memo to DTC on June 28, 2000, requesting government jurisdiction rulings for 33 night-vision commodities. The memo states that “the appropriate method for determining jurisdiction, the commodity jurisdiction process described in ITAR 120.4, has been largely ignored for certain products, according to our information.” Separately, throughout the summer and fall of 2000, DTC received technical arguments on about 28 thermal imaging/night-vision technologies from Defense. Almost 6 months later, as of December 2000, the Director of DTC established his position that the commodity jurisdiction process was the proper vehicle for these cases and informed OIG in February 2001 that letters will be sent by DTC to the affected exporters.

The government jurisdiction process failed to solve the night-vision technology controversy because there is confusion as to how the process is supposed to operate. The Director of DTC believed that the government jurisdiction process is designed to support law enforcement agencies, such as Customs. OIG believes that the confusion stems from the lack of official, written guidance for the process. Even though DTC had opened other government jurisdiction cases in FY 2000, in this instance, DTC decided that the commodity jurisdiction route was the proper way to proceed. Because this process is supposed to work in a manner similar to the commodity jurisdiction process and DTC opened 14 government jurisdiction cases in FY 2000, we believe DTC should consult with the NSC and other relevant government agencies and then write policies and procedures for the government jurisdiction process. The procedures should make it clear how the process will operate, when government agencies should use it, and the timeframes for the process.

Recommendation 7: We recommend that the Office of Defense Trade Controls establish written policies and procedures for the government jurisdiction process in coordination with all government agencies involved in the commodity jurisdiction process.

DTC partially agreed with the intent of the recommendation. They will remind other agencies and other State offices through a written notice that jurisdictional questions involving U.S. exporters must be resolved through the commodity jurisdiction procedures, while the government jurisdiction process is normally reserved for law enforcement purposes or instances in which a Federal agency seeks clarification as to equipment it has developed or owns.

EXHIBIT 14



BY FEDERAL EXPRESS

ADVANCE COPY BY ELECTRONIC MAIL

(whs.pentagon.esd.mbx.secrev@mail.mil)

September 25, 2014

Department of Defense
Office of Security Review
2A534, Pentagon
Washington DC 20301-1155

Subject: Request for OSR Review Website Content

Dear Department Representative:

This is a request for review under ITAR Section 125.4(b)(13) and DoDD 5230.29.

Accompanying this letter please find the documents for review. They consist of two (2) screenshots of an ecommerce site for a CNC product, some technical specifications and descriptions, and seven (7) images of the product in various modes of display. These documents are also attached to the email transmitting and this advance copy letter.

The original of this letter, five (5) CD-ROMs containing the electronic files, and five (5) unbound copies of the documents for review, are being sent contemporaneously herewith by Federal Express.

These documents were created by Cody Wilson, who is an employee of Defense Distributed. Defense Distributed is a Texas corporation. It is registered with the Department of State as a Defense Article Manufacturer under registration number M-34702.

The information contained in the documents is NOT company proprietary, was NOT developed under any U.S. Government contract, and is NOT subject to any government contract restrictions on dissemination.

I expect to publish the documents on a Defense Distributed owned website on or about October 1, 2014. OSR review of the documents is therefore needed before September 30, 2014, but review after this time is acceptable in lieu of return without action.

Response by email to me at crw@defdist.org is preferred. If mailing the response, the address for mailing is: 1101 West 34th St., #340, Austin, Texas 78705.

DefDist | 1101 W 34th St. # 340 Austin, TX 78705 | DefDist.org

Office of Security Review
Page 1 of 2

14-S-2590



Thank you for your consideration in the matter. I can be reached at (501) 743-9680 with any questions, comments or concerns.

Sincerely,

Cody R. Wilson
Director
Defense Distributed, Inc.

Att./Encl.:

PDF Files of Ghostgunner.net website

EXHIBIT 15



DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF PREPUBLICATION AND SECURITY REVIEW
1155 DEFENSE PENTAGON
WASHINGTON, DC 20301-1155

October 1, 2014
Ref: 14-S-2590

Mr. Cody R. Wilson
Defense Distributed
1101 West 34th Street, #340
Austin, TX 78705

Dear Mr. Wilson:

This is in response to the enclosed September 25, 2014, correspondence requesting public release approval of the enclosed document titled:

- "The Ghost Gunner"

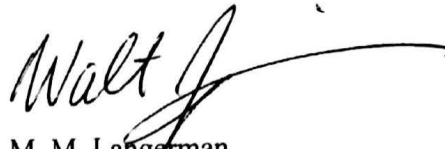
The document is **RETURNED WITHOUT ACTION**. While the Defense Office of Prepublication and Security Review (DOPSR) acknowledges your registration number (M-34702) provided in the subject correspondence as a Department of State Defense Article Manufacturer, registration does not confer any export rights or privileges. It is a precondition for the issuance or other approval for export. Defense Distributed referenced ITAR 125.4(b)(13) and DoDD 5230.09 in your review request letter. The first reference assumes your CNC machine is a defense article, and the second applies only to organizations within the Department of Defense.

DOPSR is unsure if your CNC machine itself is export-controlled as a defense article controlled under the ITAR, or is considered an accessory that the Department of Commerce would regulate under the Export Administration Regulations (15 CFR Parts 730-799). Until this determination is made DOPSR is unable to conduct the requested review under ITAR 125.4(b)(13).

Therefore, DOPSR recommends that Defense Distributed request a commodity jurisdiction (CJ) request to determine whether your CNC machine is covered by the U.S. Munitions List (USML) and therefore subject to export controls administered by the U.S. Department of State pursuant to the Arms Export Control Act and the International Traffic in Arms Regulations (ITAR).

Please direct any questions regarding this case to Mr. Donald Kluzik at 703-614-4931,
email: donald.e.kluzik.civ@mail.mil.

Sincerely,


M. M. Langerman
Chief

Enclosures:
As stated

[]

EXHIBIT 16

MATTHEW A. GOLDSTEIN, PLLC

1012 14TH STREET, NW, SUITE 620
WASHINGTON, DC 20005

VIA ELECTRONIC FILING

January 2, 2015

PM/DDTC, SA-1, 12th Floor
Office of Defense Trade Controls
Bureau of Political Military Affairs
U.S. Department of State
Washington, D.C. 20522-0012

SUBJECT: Commodity Jurisdiction Request for Ghost Gunner Machine, Plastic Mounting Jig, User Instructions, and Software (Defense Distributed, Inc., PM/DDTC Code M-34702)

Dear Sir or Madam:

Pursuant to Section 120.4 of the International Traffic in Arms Regulations (“ITAR”) (22 C.F.R. Sections 120-130), Defense Distributed requests a commodity jurisdiction determination from the Directorate of Defense Trade Controls (“DDTC”) on the Ghost Gunner machine (the “Ghost Gunner”), its plastic mounting jig, user instructions, and software for production, operation, and use of the Ghost Gunner.

The Ghost Gunner is an approximately one-foot-cubed black box that uses a drill bit mounted on a head that moves in three dimensions to automatically carve digitally-modeled shapes into polymer, wood or aluminum. It functions as a 3-axis computer-numerically-controlled (“CNC”) press that can be used to manufacture parts to firearms controlled under U.S. Munitions List (“USML”) Category I. It can also be used to manufacture items that are not controlled under the USML. The machine was designed, developed, and manufactured by Defense Distributed to automatically manufacture publicly available designs with nearly zero user interaction.

As discussed below, the Department of Defense recommended that Defense Distributed submit this commodity jurisdiction request.

Export jurisdiction over the Ghost Gunner, Jig, software, and instructions is uncertain because, although the Department of Commerce Export Administration Regulations (“EAR”) maintain a control listing for jigs, fixtures, and other metal-working items “exclusively designed for use in the manufacture of firearms” under Commerce Control List (“CCL”) Export Control Number (“ECCN”) 2B018.n, there is no corresponding carve-out for these items and related software and technical information otherwise controlled by USML Category I generally; and Category I(i) controls technical data and defense services directly related to firearms, with technical data directly related to the manufacture or production of firearms designated as Significant Military Equipment.

Please note that a letter from Defense Distributed authorizing my law firm to file this request was uploaded with this DS-4076 submission. Please direct any questions and all correspondence related to this request to my office. Communications to me at matthew@goldsteinpllc.com are preferred.

www.GoldsteinPLLC.com

I. BACKGROUND

A. Defense Distributed

Defense Distributed is a Texas corporation, registered with the Department of State under PM/DDTC Code M-34702. The company has developed technical information that can be used to produce, manufacture, and assemble various parts components, accessories, and attachments to firearms controlled under USML Category I. This includes information for the design and production of the Ghost Gunner, software necessary to operate Ghost Gunner, and code that allows production of certain items by the Ghost Gunner.¹

Following notification from DDTC in May 8, 2013, that the agency requires U.S. Government prior approval before publications of otherwise ITAR-controlled technical data into the public domain (Attachment 1), Defense Distributed has submitted requests for U.S. Government clearance of technical data to the Department of Defense Office of Prepublication and Security Review (“DOPSR”).² On October 1, 2014, DOPSR returned a Defense Distributed request for clearance of technical information on the Ghost Gunner for public release, stating that commodity jurisdiction over the item was uncertain and recommending that Defense Distributed submit a commodity jurisdiction request. See Attachment 2.

B. The Ghost Gunner

Existing CNC machines are expensive or too inaccurate to manufacture firearms for the casual user. Defense Distributed developed the Ghost Gunner to address this problem by miniaturizing the build envelope to just large enough to mill common firearm receivers, which in turn improves rigidity, reduces material cost and simultaneously relaxes certain design limits, allowing Defense Distributed to sell an inexpensive machine with more than enough accuracy to manufacture firearms.

The first design tested on the Ghost Gunner was for an AR-15 lower receiver and the Ghost Gunner was able to automatically find, align, and mill a so-called “80%” lower receiver, which was not a firearm prior to milling. The Ghost Gunner has since undergone several design revisions to reduce machine chatter, backlash, and jitter, all with the goal of keeping total design cost low.

Photographs of Ghost Gunner are provided at Attachment 3 and rendered images of the machine with the plastic jig are provided at Attachment 4.

¹ This commodity jurisdiction request seeks a determination of the code necessary to operate Ghost Gunner. It does not seek a determination on the various project files specific to production of certain items by the Ghost Gunner.

² In complying with DDTC prepublication review requirements on publication of technical information into the public domain, Defense Distributed does not intend to, nor should it be considered to, waive any defense, claim or right under law.

A schematic drawing for the Ghost Gunner is provided at Attachment 5.

Ghost Gunner form, fit, function, and performance characteristics include the following:

- It uses a compact, powder coated A36 steel frame and thick stainless T-slot rail, with preloaded ball bearings for maximum rigidity. Linear motion is achieved with low-backlash direct-drive ball screws mounted in-line with the cutting surface, thus preventing torsional gantry chatter while machining.
- It incorporates an electronic probe that automatically detects when the machine comes into contact with the work piece, allowing automatic part discovery and alignment. Ghost Gunner requires conductive parts if auto-discovery and alignment are used.
- It can manually machine nonconductive materials, but this requires manual calibration of a part to the machine - following a few simple instructions - as is required with existing CNC machines.
- Its moving parts are entirely sealed from chip debris. All bearings are sealed and contain wipers to prevent foreign contaminate entry. The rails are stainless steel and are factory lubricated, but do require periodic wiping to prolong life. End Mills dull over time and are considered a consumable.
- To contain aluminum chips, it includes a chip collection tray and all moving components are fully enclosed.
- It is capable of manufacturing deep pockets due to its horizontal gantry, which allows gravity to pull chips away from the cutting surface before they can build up and dull the end mill, as is the case on traditional CNC designs.
- It uses industry standard ER-11 collets, and ships with both 1/4" and 5/32" collets.
- It uses a standard IEC power cord and is compatible with any 110/220V circuit. No external power brick is used; the machine is entirely self-contained.
- It has two ports: Power (IEC standard) and USB (Type 'B').
- Its machinable dimensions are 140 x 75 x 60mm (~5.50 x 2.95 x 2.35")
- Its maximum part dimensions are 230 x 90 x 100mm (~9.05 x 3.50 x 3.90")
- Its overall footprint is 330 x 280mm (~13 x 11")
- Its weight is 20kg (~45 pounds)

- Its Spindle Speed is 10,000+ RPM (Final Value TBD)
- Its software requirements are Windows 7 or higher. Mac version TBD

As noted above, Ghost Gunner is capable of manufacturing more than just firearm receivers. With Defense Distributed's open source Physibles Development SDK ("pDev"), designers can distribute files via the company's '.dd' file format, which contains all installation and assembly instructions, any required jig files to hold a part in place (that users can print with a 3D printer), and all machine definitions and code to physically manufacture a particular design. To a casual user, the .dd file is a one-stop solution to manufacturing any aluminum physible that the public can design to fit into the build envelope. Defense Distributed will be developing in and supporting this format.

The .dd file format is itself open source and not constrained to the Ghost Gunner or Defense Distributed; any user can define any existing machine's specific parameters via the machine parameters list. A single file can contain specific code and installation instructions for any number of machines. A user with both a Ghost Gunner and a Tormach P1100 could manufacture a particular .dd file on either machine and manufacture the same physible with zero additional user knowledge, as only the instructions required for a particular machine are revealed to the end user. The .dd file format is a CNC response to 3D printing's universal .stl file format. However, Ghost Gunner will also accept TinyG code from any CAM program.

In operation, users provide the parts for milling. They can then simply plug their computer into the Ghost Gunner, install the Ghost Gunner software, and download any compatible .dd design file. 3D printable jigs are used to hold each part in place as each milling step is performed. For example, milling an eighty percent AR-15 lower receiver requires two jig pieces to secure the lower in place while the trigger pocket is milled, and then two more jig pieces are installed to drill the trigger pinholes. As most eighty percent firearms require deep pocket milling, Ghost Gunner's mounting table is parallel to the end mill shaft. This orientation maximizes 3D printed jig strength, minimizes jig complexity, and mechanically aligns the part to the machine upon insertion into the Maker Slide-patterned, Open Source T Slot stainless rails.

Defense Distributed expects its typical order fulfillment will contain the fully assembled Ghost Gunner CNC, plastic mounting jig designed to secure 80% AR-15 receivers, operating software and instructions. Defense Distributed also intends to place instructions and computer code needed to build and use Ghost Gunner into the public domain as Open Source technology.

Block 13 ("Sales information") is not provided with this request because the Ghost Gunner is still in development as Defense Distributed awaits arrival of various production pieces and continues to make any required changes to the product. As such, the company has not yet delivered any machines (i.e., no completed sales). However, the company has accepted 469 pre-orders and 413 advance deposits from prospective purchasers. Each of these orders, except for one, are intended for domestic sale. In addition, consistent with U.S. law, final sales will carry conditions that limit purchases to private use (i.e., not for commercial or military use).

C. User Instructions and Operating Software for the Ghost Gunner

The current draft User Instructions for the Ghost Gunner accompanies this commodity jurisdiction request at Attachment 6. It contains information on how to attach a “80%” lower receiver to Ghost Gunner, such that Ghost Gunner can mill and drill all required holes to transform the lower receiver into a firearm. Ghost Gunner presents numerous User Instructions, User Graphics, and User Selections to the operator. Ghost Gunner performs work via Calibration Code and Milling Code. Ghost Gunner also assists the user in creating 3D printable Jigs, if needed.

The software necessary to produce and operate the Ghost Gunner includes AutoDesk Inventor and a simple executable application that can interpret CNC part files and TinyG code. Additional information detailing the purpose, function, and capability of the software, as requested by DDTC’s DS-4076 Commodity Jurisdiction (CJ) Guidance for Software, accompanies this commodity jurisdiction request at Attachment 7.

II. COMMODITY JURISDICTION STANDARD

The standard applicable to Department of State and other agency considerations of commodity jurisdiction is set forth at ITAR Section 120.3. ITAR Subsection 120.3(a) extends Department of State jurisdiction to any item that meets the criteria of a defense article described on the USML or that provides equivalent performance capabilities; and ITAR Section 120.3(b) provides that a specific article not presently described on the USML shall be determined in the future as a defense article if it provides a critical military or intelligence advantage.

A. Relevant USML Control Listings

Subparagraph (h) to USML Category I controls components, parts, accessories, and attachments for firearms to .50 caliber inclusive. The Ghost Gunner does not meet the Category I(h) criteria because it is not a component or part to a firearm. Rather, it is a machine that can be used for the manufacture of such articles.

Subparagraph (i) to USML Category I controls technical data, to include “software” as defined at Section 120.45(f), and defense services directly related to the firearms and components, parts, accessories, and attachments for firearms to .50 caliber inclusive. Technical data directly related to the manufacture or production of firearms controlled in Category I is designated as Significant Military Equipment.

The USML does not contain a control listing that describes items used for the manufacture of firearms. Instead, that listing is contained on the EAR Commerce Control List (“CCL”) entry for ECCN 2B018.n, which controls “Jigs and fixtures and other metal-working implements or “accessories” of the kinds exclusively designed for use in the manufacture of firearms. ECCN 2D018 controls software” for the “development”, “production” or “use” of equipment controlled by 2B018; and ECCN 2E018, in turn, controls “Technology” for the “use” of equipment controlled by 2B018.

The scope of the CCL controls on firearms manufacturing equipment and technology is unclear because the EAR only controls items not described on the USML and Category I does not contain any carve-out from ITAR control for software or technology controlled under ECCNs 2D018 and 2E018. To the contrary, if literally applied, USML Category I(i) treats such technical information as Significant Military Equipment.

Because there is no specific carve-out in Category I or elsewhere in the USML for software or technology controlled by 2D018 and 2E018, it is very difficult to distinguish between technical data for the manufacture or production of firearms controlled in Category I and technology for the development, production, and use of equipment used to manufacture firearms controlled at 2D018 and 2E018. This is a primary concern of the present commodity jurisdiction request.

Nevertheless, EAR control is consistent with U.S. Implementation of Wassenaar Controls. Specifically, ECCNs 2B018, ECCN 2E018, and 2B018 are Wassenaar Arrangement-based controls, subject to the National Security reason for control and which correspond to Category 2 of the Wassenaar Arrangement List of Dual-Use Items. In fact, 2B018 is titled, "Equipment on the Wassenaar Arrangement Munitions List."

Although relevant text of the ITAR and EAR control listings lack clarity, it appears that the U.S. Government decided to implement export controls on firearms manufacturing equipment and associated technical information in the EAR when it first implemented the Wassenaar Arrangement controls for such items. Accordingly, Defense Distributed believes that the Ghost Gunner does not meet criteria of a defense article described on the USML and that it does not provide equivalent performance capabilities to an article described on the USML.

Defense Distributed further notes that the DDTC should consider amending USML Category I to provide an express carve-out for EAR items controlled under ECCNs 2B018.n, ECCN 2E018, and 2B018. Alternatively, if DDTC intends to control firearms manufacturing equipment under the USML, it should make this clear in the regulations. Towards this end, any determination on the instant request that imposes ITAR control should be widely disseminated and shared with the firearms manufacturing industry.

B. Ghost Gunner Does Not Provide a Critical Military or Intelligence Advantage.

As noted above, ITAR Section 120.3(b) provides that a specific article not presently described on the USML shall be determined in the future as a defense article if it provides a critical military or intelligence advantage.

The function and performance of the Ghost Gunner does not provide a critical military or intelligence advantage. Rather, it is essentially a jig press based on a simple design that is easily replicated by any skilled machinist. In fact, the Ghost Gunner can be produced by persons with no formal engineering background.

In addition, Ghost Gunner builds on technology readily available in the Open Source community, including the gshield 3 axis motion hardware (<http://synthetos.myshopify.com/products/gshield-v5>), the grbl g-code parser and motion controller (<https://github.com/grbl/grbl>), and the Arduino microcontroller (<http://arduino.cc>).

Further, instructions and/or electronic files for production of jig presses with similar form, fit, and function to the Ghost Gunner are publicly available for download at a variety of web addresses, to include the following:

<http://aresarmor.com/store/Item/Polymer-80-Black>
<http://www.thingiverse.com/thing:160266>
https://github.com/DefiantCad/defcad-repo/tree/master/Rifles/AR-15_80_percent_lower_v5-shadowfall/AR-15_80_percent_Lower_Drill_Jig_v1-Shadowfall
<http://www.advancedrifles.com/3d-printed-jig-version-2-0/>
<http://www.80percentarms.com/products/80-ar-15-easy-jig>
<http://www.sierranevadaarms.com/jig.pdf>
<http://www.rockethub.com/projects/24384-80-lower-receiver-ar15-ar10-rudius-1911>

III. CONCLUSION

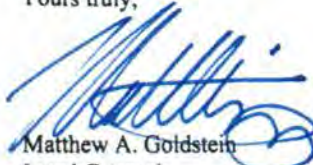
Considering the apparent intent of the U.S. Government in implementing relevant Wassenaar Arrangement controls in the EAR, Defense Distributed believes that the Ghost Gunner does not meet the criteria of an article described on the USML. In addition, the Ghost Gunner does not provide a critical military or intelligence advantage. Accordingly, Defense Distributed respectfully requests that the Department of State issue a commodity jurisdiction determination stating that the Ghost Gunner, its plastic mounting jig, operating software, and production and operation instructions do not meet the criteria of ITAR 120.3 and are subject to Department of Commerce jurisdiction under the EAR.

Defense Distributed authorizes the release for general publication of the information contained in Block 5 of the DS-4076 Form. However, other information in this request and documents submitted with Defense Distributed's DS-4076 Submission contain sensitive business information that is proprietary, confidential, and exempt from disclosure under the Freedom of Information Act, 5 U.S.C. Section 552, and is also protected under the Trade Secrets Act, 18 U.S.C. Section 1905. Accordingly, pursuant to ITAR Section 130.15, Defense Distributed requests that information in this submission other than that contained in Block 5 be withheld in the event of a request for its disclosure.

Commodity Jurisdiction Request
January 2, 2015
Page 8 of 9

Thank you for your prompt attention to this matter and please contact me at 202-550-0040 or at matthew@goldsteinpllc.com if any additional information is needed.

Yours truly,


Matthew A. Goldstein
Legal Counsel

COMPANY CERTIFICATION:

Cody Wilson, the Principal of Defense Distributed, certifies that he is the duly authorized representative of Defense Distributed; and that in such capacity, he certifies that he has carefully read the foregoing Commodity Jurisdiction request; and that the contents of the request are true and correct to the best of his knowledge, information and belief after reasonable inquiry into the matters discussed.


Signature

1/2/2015
Date

ATTACHMENTS TO LETTER OF EXPLANATION:

- | | |
|--------------|--|
| Attachment 1 | May 8, 2013 DDTC Letter to Defense Distributed |
| Attachment 2 | October 1, 2014 DOPSR Letter to Defense Distributed |
| Attachment 3 | Photographs of Ghost Gunner Machine |
| Attachment 4 | Rendered Images of Ghost Gunner Machine |
| Attachment 5 | Ghost Gunner Schematics |
| Attachment 6 | Ghost Gunner User Instructions |
| Attachment 7 | Answers to DS-4076 Commodity Jurisdiction (CJ) Guidance for Software |

www.GoldsteinPLLC.com

Electronic Form Version Number: 1.2
For DDTC Use Only
CJ Number: _____

OMB APPROVAL NO. 1405-0163
EXPIRATION DATE: 01/31/2013
*ESTIMATED BURDEN: 10 Hours

U.S. Department of State

DS-4076 Commodity Jurisdiction (CJ) Determination Form

*PAPERWORK REDUCTION ACT STATEMENT: Public reporting burden for this collection of information is estimated to average 10 hours per response, including time required for searching existing data sources, gathering the necessary data, providing the information required, and reviewing the final collection. Send comments on the accuracy of this estimate of the burden and recommendations for reducing it to: Department of State (A/GIS/DIR) Washington, D.C. 20520.

A. Applicant Information

1. Applicant's Information: (Select all that apply)

Applicant is: ☐ Government ☒ Manufacturer ☒ Exporter ☐ Manufacturer's Representative ☐ Other

Applicant Name: (Company, Organization) Defense Distributed, Inc.

Address: 1101 W 34th St. #340

City: Austin

State: TX

Zip Code: 78705

Phone #: 501-743-9680

PM/DDTC Registrant Code: M-3470

(If applicable)

Add Item

Remove Item #: 1

Name: (Point of Contact) Cody R. Wilson

Phone #: 501-743-9680

Fax #: _____

Email: crw@defdist.org

2. Submitter Information if other than Applicant in Block 1: (Complete if applicable)

Submitter Name: (Company, Organization) Matthew A. Goldstein, PLLC

Address: 1012 14th Street, NW, Suite 620

City: Washington

State: DC

Zip Code: 20005

Phone #: 202-550-0040

PM/DDTC Registrant Code: _____

(If applicable)

Add Item

Remove Item #: 1

Name: (Point of Contact) Matthew A. Goldstein

Phone #: 202-550-0040

Fax #: _____

Email: matthew@goldsteinpllc.com

☒ Attachment: Authorization from Applicant to Submitter authorizing submitter to file on its behalf and to release information in Block 5.

B. Transaction Description and Compliance Information

3. Transaction Description: (Note: No request involving Classified information will be considered.)

This Application Represents:

a. ☒ New Request

b. ☐ Resubmission

Prior CJ Case Number: _____

☐ Returned Without Action (RWA)

☐ Reconsideration (Include Prior CJ Determination Case Number)

Summarize Reason for Resubmission (limited to 1200 characters)

Related to Compliance Matter (limited to 1200 characters)

☐ Yes ☒ No

If yes, provide disclosure and/or case number (if available) and details to include U.S. Government Point of Contact. If status changes advise DDTC.

DDTC Compliance has an open matter related to certain files posted in the public domain by Defense Distributed in 2012. However, the product and files that are the subject of this instant commodity jurisdiction request are different than the files that are subject to the DDTC compliance matter.

C. Commodity Description

4. Select Commodity Type: (Select all that apply) (22 C.F.R. 120.9, 120.10 and 121.8)

☒ End Item

☐ Component/Major

☐ Component/Minor

☐ Part

☒ Accessory/Attachment

☒ Software

☐ Firmware

☐ Services

☐ System

☒ Information or Technical Data

5. Commodity/Service Information: (Note: Complete all that apply and if not applicable, enter "N/A".)

a. Product Name: Ghost Gunner Machine, Plastic Mounting Jig, User Instructions, and Software

b. Model/Version Number: N/A

c. Part Number: N/A

d. National Stock Number: N/A

e. Other Identifier: (If applicable) N/A

f. Manufacturer: Defense Distributed, Inc.

g. Service: N/A

h. Generic Description: Ghost Gunner

i. Manufacturer's Website: https://defdist.org

j. Commodity/Service Website: https://www.ghostgunner.net

Note: Only one commodity may be entered; variants require separate submission. However, variants of a commodity or a family of commodities closely related, that is, major characteristics and descriptive information of the commodity are essentially the same and would be included in the same U.S. Munitions List category and subcategory may be considered.

6. Additional Commodity Information/Documentation:
 (Brochures, Technical Information, Drawings, Schematics, Blue Prints, Course Syllabus/Handouts, Training Materials.) Attach product datasheet or other technical information such that an informed technical evaluation is possible.) Note: cost in U.S. Dollars. If unit is not listed in drop down list, e.g. service or training, enter the commodity.

a. Cost Per Unit: \$1,299.00 Units

b. Documentation Attached: ☒

c. Patent Information:

7. Commodity/Service Description: (limited to 1200 characters)
 Brief summary of commodity or service (e.g. component used in aircraft communication system). Describe the product's use (what it does, how it operates, the components/system in which it is used and all current uses). Specify if commodity/service is controlled or restricted for public release by U.S. Government.

Ghost Gunner Machine, Plastic Mounting Jig, User Instructions, and Software

8. Identify any special and/or unique characteristics/capabilities: (Mark all boxes that apply and provide explanation/description)

a. ☐ Designed to military or intelligence standards or specifications.

b. ☐ Designed for military application.

c. ☐ Special characteristics (e.g. radiation-hardening, ballistic protection, hard points, TEMPEST capability, thermal or infrared signature reduction capability, surveillance or intelligence gathering capability).

d. ☐ Commercial item modified for military application, provide nomenclature and model number to differentiate from commercial item.

e. ☐ Commercial item modified for military application, state specific distinct difference between original commercial item and modified item.

f. ☐ Services (provide comparable information as that which provided above and by marking this box, indicate it is for services versus hardware).

Explanation/Description (If the product is included in a higher assembly or end item, identify each higher assembly or end item that incorporates the product and its use. Identify all military applications and military capabilities of the product, and any equivalent products used for military application.) Summarize technical details of special characteristics (e.g. if image intensification tubes, provide level of technology, such as Gen II, Gen III, etc.). (limited to 600 characters)

D. Product Origin

9. Military/Commercial Modification of Commodity:

a. Was this commodity originally specifically designed or developed for a military use?
☐ Yes ☒ No

b. Was this commodity originally civil and subsequently adapted, configured or modified for a military use?
☐ Yes ☒ No

c. Was this commodity originally military and subsequently adapted, reconfigured or modified for commercial use?
☐ Yes ☒ No

d. Specifically define the modifications/changes and capabilities added to the commodity. List any differences in form, fit and/or function between the modified and unmodified versions: (limited to 600 characters)

Ghost Gunner builds on technology readily available in the Open Source community, including the gshield 3 axis motion hardware (<http://synthetos.myshopify.com/products/gshield-v5>), the grbl g-code parser and motion controller (<https://github.com/grbl/grbl>), and the Arduino microcontroller (<http://arduino.cc>). The Ghost Gunner can be used to manufacture items controlled by the EAR or ITAR.

☒ Supporting Documentation Attached

10. Status of Product Development: (Mark the status of the product and provide an explanation/description)

a. ☒ In Development

b. ☒ In Use

Explanation/Description (limited to 4000 characters)

The Ghost Gunner is in final stages of development as Defense Distributed awaits arrival of various production pieces and continues to make any required changes to the product. As such, Defense Distributed has not yet delivered any machines for sale. However, the Ghost Gunner prototypes (see product pictures and rendered image attachments) are used by the company in testing and product development.

☒ Supporting Documentation Attached

11. Funding History: (Check all that apply)
 Include funding source contract or subcontract number and supporting documentation.

a. ☐ USG Agency

b. ☐ Foreign Government Agency

c. ☐ U.S. or Foreign Contractor

d. ☒ Self Funded


e. ☐ University Funded

Explanation/Description (limited to 600 characters) <div style="border: 1px solid black; height: 20px; width: 100%;"></div>	
<input type="checkbox"/> Supporting Documentation Attached	
12. U.S. and/or Foreign Availability of Identical Products: (Enter Foreign Export Controls, if known)	
<input type="checkbox"/> None	
<div style="border: 1px solid black; padding: 2px 5px; background-color: #f0f0f0;">Add Item</div>	
<div style="border: 1px solid black; padding: 2px;">Remove Item #: 1</div>	
Manufacturer: _____ Commodity: _____ Model #: _____ In Use/In Development: _____ Foreign Exports Control: _____ Manufacturer's Website: _____ Explanation/Description (limited to 600 characters) <div style="border: 1px solid black; height: 20px; width: 100%;"></div>	
<input type="checkbox"/> Supporting Documentation Attached	
E. Sales Information	
13. Sales Information: (Select One) (See Block 13 Template) Military and commercial sales data must be provided, as well as listing of the military and commercial customers. The information pertains specifically to the commodity/service in Block 8. Complete the attachment, if applicable. (Note: Submit one single file up to 35MB with sales information. Do not separate the sales information into multiple smaller files.)	
<input type="checkbox"/> Sales Information Attachment (Template "Block 13 Sales Information") Attached <input checked="" type="checkbox"/> No Sales	
F. Miscellaneous Information	
14. Has this Commodity been: (limited to 100 characters)	
a. Has this Commodity been Previously Exported <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No <input type="checkbox"/> Unknown If yes, cite U.S. Government licensing jurisdiction and provide license number, if applicable. <div style="border: 1px solid black; height: 20px; width: 100%;"></div>	
b. Has this Commodity been the subject of a Prior CJ? <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No <input type="checkbox"/> Unknown If yes, Cite CJ Number. (Applicant should list any prior CJ even if not submitted by them, e.g., submitted by Original Equipment Manufacturer (OEM), by the U.S. Government or by a third party.) <div style="border: 1px solid black; height: 20px; width: 100%;"></div>	
c. Has this Commodity been subject to a Department of Commerce Classification Request? <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No <input type="checkbox"/> Unknown If yes, cite U.S. Government licensing jurisdiction and if under Department of Commerce, attach a copy with Export Control Classification Number (ECCN). <div style="border: 1px solid black; height: 20px; width: 100%;"></div>	
d. Has this Commodity been Exported under a Foreign Military Sale (FMS) case? <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No <input type="checkbox"/> Unknown If yes, cite Foreign Military Sale (FMS) case number. <div style="border: 1px solid black; height: 20px; width: 100%;"></div>	
15. Description of the commodity and final DDTC action will be posted on the DDTC website for public access based on the information provided in Block 5 and any other descriptive information provided below. If you believe that any information contained in Block 5 is proprietary, please specifically identify the information below and provide summarized rationale for DDTC to consider withholding the information from public notice: (Limited to 600 characters. Additional justification may be provided as an attachment.) <div style="border: 1px solid black; padding: 5px;"> Ghost Gunner Machine, Plastic Mounting Jig, User Instructions, and Software </div>	
16. Reason for Submitting CJ: (limited to 600 characters) <div style="border: 1px solid black; padding: 5px;"> To resolve uncertainty as to whether subject to Department of State or Department of Commerce export control. </div>	
17. Suggested U.S. Munitions List or Commerce Control List Number:	
a. U.S. Munitions List (22 C.F.R. 121) Category/Sub Category <div style="border: 1px solid black; height: 20px; width: 100%;"></div>	
b. Export Administration Regulations (15 C.F.R. 730-774), Export Control Classification Number <div style="border: 1px solid black; padding: 2px;"> 2B018, 2D018, 2E018 </div>	
18. Other Miscellaneous Information to be Considered that is not Otherwise Included in this Form: (e.g. U.S. Government Agency and point of contact information.) (limited to 300 characters) <div style="border: 1px solid black; padding: 5px;"> Ghost Gunner Schematics, Pictures, Rendered Images, and Software Supplement </div>	
<input checked="" type="checkbox"/> Supporting Documentation Attached	

G. Applicant/Submitter's Certification**19. Applicant/Submitter's Certification:** Note: ONLY this one page must be printed, signed, and scanned as an attachment.

Under Penalty According to Federal Law (See 22 CFR 127, 22 U.S.C. 2778, and 22 U.S.C. 1001).

I am the authorized employee of the company cited in Block 1, or a third party as described in Block 2 authorized to submit on behalf of the company in Block 4, and certify as to the accuracy and completeness of the information provided and have not knowingly omitted information that could have an impact on the final determination issued by the U.S. Department of State. Furthermore, I have specific authority to release for publication the text contained in Block 5.


Signature _____ Cody R. Wilson _____ Printed Name _____ 01/02/2015 _____ Date

☒ By checking this box, Applicant authorizes DOTC to email the Commodity Jurisdiction determination as well as any other information associated with this case. The Commodity Jurisdiction determination will be mailed to the address below if box is not checked.

Name: Cody R. Wilson
Title: DIRECTOR
Company: DEFENSE DISTRIBUTED
Address: 1101 W 34TH ST #540
City: AUSTIN State: TX Zip Code: 78705
Phone #: (501) 743-9680 Email: _____

EXHIBIT 17



United States Department of State

Bureau of Political-Military Affairs

Directorate of Defense Trade Controls

Washington, D.C. 20522-0112

In Reply refer to
DDTC Case CJ 1083-14 (RE-ISSUE)

APR 15 2015

YOUR SUBMISSION DATED: January 2, 2015

COMMODITY JURISDICTION DETERMINATION FOR: Ghost Gunner Machine, Plastic Mounting Jig, User Instructions, and Software

The product described in your submission is a one cubic foot box that functions as a 3-axis, computer-numerically-controlled (CNC) press capable of automatically milling parts out of various materials through software designs.

A technical review of your commodity jurisdiction (CJ) request has been concluded by the requisite agencies of the United States Government. A split jurisdiction determination of this request has been determined, as follows:

The Department of State has determined that the **Ghost Gunner, its plastic mounting jig, operating software, and production and operation instructions are not subject to the jurisdiction of the Department of State.** However, export may require authorization from the Department of Commerce (DOC). Please consult the DOC Office of Exporter Services at (202) 482-4811 to make a Classification Request (CCATS) and satisfy other applicable requirements prior to export.

The Department of State has determined that the **project files, data files, or any form of technical data for producing a defense article, including an 80% AR-15 lower receiver, are subject to the jurisdiction of the Department of State in accordance with the International Traffic in Arms Regulations (ITAR) (22 CFR 120 through 130).** They are

Continued on Page Two

Cody R. Wilson
Defense Distributed, Inc.
1101 W 34th Street, #340
Austin, TX 78705
crw@defdist.org

DOSWASHINGTONSUP00178

Page Two

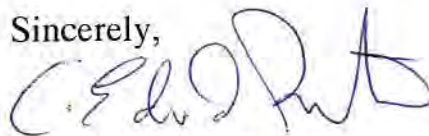
In Reply refer to
DDTC Case CJ 1083-14

designated as technical data under Category I(i) of the United States Munitions List (USML). A license or other approval is required pursuant to the ITAR prior to any export or temporary import.

Should you not agree with this determination and have additional facts not included in the original submission, you may submit a new CJ request. If you do not agree with this determination and have no additional facts to present, you may request that this determination be reviewed by the Deputy Assistant Secretary of State for Defense Trade Controls.

Should you require further assistance on this matter, please contact Samuel Harmon at (202) 663-2811 or HarmonSC@state.gov.

Sincerely,



C. Edward Peartree

Director

Office of Defense Trade Controls Policy

Cc: Matthew A. Goldstein
1012 14th Street, NW, Suite 620
Washington, DC 20005
matthew@goldsteinpllc.com

EXHIBIT 18



BY FEDERAL EXPRESS

ADVANCE COPY BY ELECTRONIC MAIL

(whs.pentagon.esd.mbx.secrev@mail.mil)

September 2, 2014

Department of Defense
Office of Security Review
2A534, Pentagon
Washington DC 20301-1155

Subject: Request for OSR Review of AR-15 Lower Receiver Documents

Dear Department Representative:

This is a request for review under ITAR Section 125.4(b)(13) and DoDD 5230.29.

Accompanying this letter please find the documents for review. They consist of two (2) electronic files (.STP, and .STL formats) for a lower receiver to the AR-15 rifle and five (5) rendered images of the electronic files. These documents are also attached to the email transmitting and advance copy of this letter.

The original of this letter, five (5) CD-ROMs containing the electronic files, and five (5) unbound copies of the rendered images for review, are being sent contemporaneously herewith by Federal Express.

The electronic files are Computer Assisted Drafting ("CAD") files that can be used with a 3D printer or a computer numerical control machine to produce the hardware depicted in the rendered images of the electronic files.

These documents were created by John Sullivan, who is an employee of Defense Distributed. Defense Distributed is a Texas corporation. It is registered with the Department of State as a Defense Article Manufacturer under registration number M-34702.

The information contained in the documents is NOT company proprietary, was NOT developed under any U.S. Government contract, and is NOT subject to any government contract restrictions on dissemination.

These documents are NOT in the public domain. However, public release of the information contained in documents will not harm national security because design

DefDist | 1101 W 34th St. # 340 Austin, TX 78705 | DefDist.org

Office of Security Review
Page 1 of 3



specifications containing similar information and similar CAD files for AR-15 lower receivers are already publicly available online.

.STP and/or .STL files for AR-15 lower receivers are already publicly available for download at a variety of web addresses, to include the following:

www.3dcadbrowser.com/download.aspx?3dmodel=42013
<http://grabcad.com/library/ar-15-lower-receiver>
<http://grabcad.com/library/a-printable-ar15-lower-receiver>
<https://grabcad.com/library/ar15-lower-concept-1>
<http://grabcad.com/library/ar-15-lower-receiver>

Other CAD file formats for lower receivers to the AR-15 are also publicly available online at web addresses, to include the following:

www.3dcadbrowser.com/download.aspx?3dmodel=42013
www.cncguns.com/downloads.html

In addition, detailed design specifications for AR-15 lower receivers are also available online from a variety of sources, to include the following:

www.homegunsmith.com/archive/T6215.html
www.ar15.com/archive/topic.html?b=3&f=4&t=619878
www.advancedrifles.com/build-it-yourself
www.biggerhammer.net/ar15/cad/

I expect to publish the documents on the Defense Distributed website on or about October 1, 2014. OSR review of the documents is therefore needed before September 30, 2014, but review after this time is acceptable in lieu of return without action.

Response by email to me at crw@defdist.org is preferred. If mailing the response, the address for mailing is: 1101 West 34th St., #340, Austin, Texas 78705.

Thank you for your consideration in the matter. I can be reached at (501) 743-9680 with any questions, comments or concerns.

Sincerely,

Cody R. Wilson
Director
Defense Distributed, Inc.

DefDist | 1101 W 34th St. # 340 Austin, TX 78705 | DefDist.org

Office of Security Review
Page 2 of 3



Att./Encl.:

.IPT Electronic File for AR-15 Lower Receiver (CD-ROM)
.STEP Electronic File for AR-15 Lower Receiver (CD-ROM)
.STL Electronic File for AR-15 Lower Receiver (CD-ROM)
5 Rendered Images of .STEP and .STL files

I

I

EXHIBIT 19



BY FEDERAL EXPRESS

ADVANCE COPY BY ELECTRONIC MAIL

(whs.pentagon.esd.mbx.secrev@mail.mil)

October 9, 2014

Department of Defense
Office of Security Review
2A534, Pentagon
Washington DC 20301-1155

Subject: Request for OSR Review of AR-15 Lower Receiver Documents (C)

Dear Department Representative:

This is a request for review under ITAR Section 125.4(b)(13) and DoDD 5230.29.

Accompanying this letter please find the documents for review. They consist of two (2) electronic files (.STP, and .STL formats) for a lower receiver to the AR-15 rifle and five (5) rendered images of the electronic files. These documents are also attached to the email transmitting and this advance copy letter.

The original of this letter, five (5) CD-ROMs containing the electronic files, and five (5) unbound copies of the rendered images for review, are being sent contemporaneously herewith by Federal Express.

The electronic files are Computer Assisted Drafting ("CAD") files that can be used with a 3D printer or a computer numerical control machine to produce the hardware depicted in the rendered images of the electronic files.

These documents were created by John Sullivan, who is an employee of Defense Distributed. Defense Distributed is a Texas corporation. It is registered with the Department of State as a Defense Article Manufacturer under registration number M-34702.

The information contained in the documents is NOT company proprietary, was NOT developed under any U.S. Government contract, and is NOT subject to any government contract restrictions on dissemination.

These documents are NOT in the public domain. However, public release of the information contained in documents will not harm national security because design

DefDist | 1101 W 34th St. # 340 Austin, TX 78705 | DefDist.org

Office of Security Review
Page 1 of 3



specifications containing similar information and similar CAD files for AR-15 lower receivers are already publicly available online.

.STP and/or .STL files for AR-15 lower receivers are already publicly available for download at a variety of web addresses, to include the following:

www.3dcadbrowser.com/download.aspx?3dmodel=42013
<http://grabcad.com/library/ar-15-lower-receiver>
<http://grabcad.com/library/a-printable-ar15-lower-receiver>
<https://grabcad.com/library/ar15-lower-concept-1>
<http://grabcad.com/library/ar-15-lower-receiver>

Other CAD file formats for lower receivers to the AR-15 are also publicly available online at web addresses, to include the following:

www.3dcadbrowser.com/download.aspx?3dmodel=42013
www.cncguns.com/downloads.html

In addition, detailed design specifications for AR-15 lower receivers are also available online from a variety of sources, to include the following:

www.homegunsmith.com/archive/T6215.html
www.ar15.com/archive/topic.html?b=3&f=4&t=619878
www.advancedrifles.com/build-it-yourself
www.biggerhammer.net/ar15/cad/

I expect to publish the documents on the Defense Distributed website on or about October 1, 2014. OSR review of the documents is therefore needed before November 3, 2014, but review after this time is acceptable in lieu of return without action.

Response by email to me at crw@defdist.org is preferred. If mailing the response, the address for mailing is: 1101 West 34th St., #340, Austin, Texas 78705.

Thank you for your consideration in the matter. I can be reached at (501) 743-9680 with any questions, comments or concerns.

Sincerely,

Cody R. Wilson
Director
Defense Distributed, Inc.

DefDist | 1101 W 34th St. # 340 Austin, TX 78705 | DefDist.org

Office of Security Review
Page 2 of 3



Att./Encl.:

.STP Electronic File for AR-15 Lower Receiver (Collapsible Stock) (CD-ROM)
.STL Electronic File for AR-15 Lower Receiver (Collapsible Stock) (CD-ROM)
5 Rendered Images of .STP and .STL files

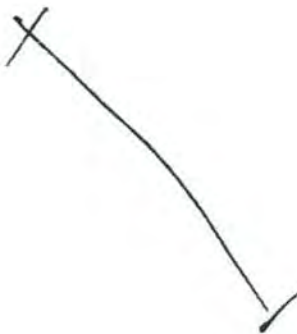


EXHIBIT 20



BY FEDERAL EXPRESS

ADVANCE COPY BY ELECTRONIC MAIL

(whs.pentagon.esd.mbx.secrev@mail.mil)

October 9, 2014

Defense Office of Prepublication and Security Review
Room 2A534
1155 Defense Pentagon
Washington DC 20301-1155

Subject: Request for OSR Review of AR-15 Lower Receiver Documents (M)

Dear Department Representative:

This is a request for review under ITAR Section 125.4(b)(13) and DoDD 5230.29.

Accompanying this letter please find the documents for review. They consist of two (2) electronic files (.STP, and .STL formats) for a lower receiver to the AR-15 rifle and five (5) rendered images of the electronic files. These documents are also attached to the email transmitting and this advance copy letter.

The original of this letter, five (5) CD-ROMs containing the electronic files, and five (5) unbound copies of the rendered images for review, are being sent contemporaneously herewith by Federal Express.

The electronic files are Computer Assisted Drafting ("CAD") files that can be used with a 3D printer or a computer numerical control machine to produce the hardware depicted in the rendered images of the electronic files.

These documents were created by John Sullivan, who is an employee of Defense Distributed. Defense Distributed is a Texas corporation. It is registered with the Department of State as a Defense Article Manufacturer under registration number M-34702.

The information contained in the documents is NOT company proprietary, was NOT developed under any U.S. Government contract, and is NOT subject to any government contract restrictions on dissemination.

These documents are NOT in the public domain. However, public release of the information contained in documents will not harm national security because design



specifications containing similar information and similar CAD files for AR-15 lower receivers are already publicly available online.

.STP and/or .STL files for AR-15 lower receivers are already publicly available for download at a variety of web addresses, to include the following:

www.3dcadbrowser.com/download.aspx?3dmodel=42013
<http://grabcad.com/library/ar-15-lower-receiver>
<http://grabcad.com/library/a-printable-ar15-lower-receiver>
<https://grabcad.com/library/ar15-lower-concept-1>
<http://grabcad.com/library/ar-15-lower-receiver>

Other CAD file formats for lower receivers to the AR-15 are also publicly available online at web addresses, to include the following:

www.3dcadbrowser.com/download.aspx?3dmodel=42013
www.cncguns.com/downloads.html

In addition, detailed design specifications for AR-15 lower receivers are also available online from a variety of sources, to include the following:

www.homegunsmith.com/archive/T6215.html
www.ar15.com/archive/topic.html?b=3&f=4&t=619878
www.advancedrifles.com/build-it-yourself
www.biggerhammer.net/ar15/cad/

I expect to publish the documents on the Defense Distributed website on or about October 1, 2014. OSR review of the documents is therefore needed before November 3, 2014, but review after this time is acceptable in lieu of return without action.

Response by email to me at crw@defdist.org is preferred. If mailing the response, the address for mailing is: 1101 West 34th St., #340, Austin, Texas 78705.

Thank you for your consideration in the matter. I can be reached at (501) 743-9680 with any questions, comments or concerns.

Sincerely,

A handwritten signature in black ink, appearing to read "Cody R. Wilson".

Cody R. Wilson
Director
Defense Distributed, Inc.

DefDist | 1101 W 34th St. # 340 Austin, TX 78705 | DefDist.org

Office of Security Review
Page 2 of 3



Att./Encl.:

.STP Electronic File for AR-15 Lower Receiver (Metal) (CD-ROM)
.STL Electronic File for AR-15 Lower Receiver (Metal) (CD-ROM)
5 Rendered Images of .STP and .STL files

EXHIBIT 21



BY FEDERAL EXPRESS

ADVANCE COPY BY ELECTRONIC MAIL

(whs.pentagon.esd.mbx.secrev@mail.mil)

October 23, 2014

Defense Office of Prepublication and Security Review
Room 2A534
1155 Defense Pentagon
Washington DC 20301-1155

Subject: Request for OSR Review of AR-15 Lower Receiver Documents (C)

Dear Department Representative:

This is a request for review under ITAR Section 125.4(b)(13) and DoDD 5230.29.

Accompanying this letter please find the documents for review. They consist of two (2) electronic files (.STP, and .STL formats) for a lower receiver to the AR-15 rifle and five (5) rendered images of the electronic files. These documents are also attached to the email transmitting and this advance copy letter.

The original of this letter, five (5) CD-ROMs containing the electronic files, and five (5) unbound copies of the rendered images for review, are being sent contemporaneously herewith by Federal Express.

The electronic files are Computer Assisted Drafting ("CAD") files that can be used with a 3D printer or a computer numerical control machine to produce the hardware depicted in the rendered images of the electronic files.

These documents were created by John Sullivan, who is an employee of Defense Distributed. Defense Distributed is a Texas corporation. It is registered with the Department of State as a Defense Article Manufacturer under registration number M-34702.

The information contained in the documents is NOT company proprietary, was NOT developed under any U.S. Government contract, and is NOT subject to any government contract restrictions on dissemination.

These documents are NOT in the public domain. However, public release of the information contained in documents will not harm national security because design



specifications containing similar information and similar CAD files for AR-15 lower receivers are already publicly available online.

.STP and/or .STL files for AR-15 lower receivers are already publicly available for download at a variety of web addresses, to include the following:

www.3dcadbrowser.com/download.aspx?3dmodel=42013
<http://grabcad.com/library/ar-15-lower-receiver>
<http://grabcad.com/library/a-printable-ar15-lower-receiver>
<https://grabcad.com/library/ar15-lower-concept-1>
<http://grabcad.com/library/ar-15-lower-receiver>

Other CAD file formats for lower receivers to the AR-15 are also publicly available online at web addresses, to include the following:

www.3dcadbrowser.com/download.aspx?3dmodel=42013
www.cncguns.com/downloads.html

In addition, detailed design specifications for AR-15 lower receivers are also available online from a variety of sources, to include the following:

www.homegunsmith.com/archive/T6215.html
www.ar15.com/archive/topic.html?b=3&f=4&t=619878
www.advancedrifles.com/build-it-yourself
www.biggerhammer.net/ar15/cad/

I expect to publish the documents on the Defense Distributed website on or about October 1, 2014. OSR review of the documents is therefore needed before November 3, 2014, but review after this time is acceptable in lieu of return without action.

Response by email to me at crw@defdist.org is preferred. If mailing the response, the address for mailing is: 1101 West 34th St., #340, Austin, Texas 78705.

Thank you for your consideration in the matter. I can be reached at (501) 743-9680 with any questions, comments or concerns.

Sincerely,

A handwritten signature in black ink, appearing to read "Cody R. Wilson", with a long horizontal flourish extending to the right.

Cody R. Wilson
Director
Defense Distributed, Inc.



Att./Encl.:

.STP Electronic File for AR-15 Lower Receiver (Collapsible Stock) (CD-ROM)
.STL Electronic File for AR-15 Lower Receiver (Collapsible Stock) (CD-ROM)
5 Rendered Images of .STP and .STL files

EXHIBIT 22

From: King, Walter J CIV WHS ESD (US) walter.j.king.civ@mail.mil
Subject: RE: Meeting re Open Defense Distributed Requests
Date: December 31, 2014 at 2:59 PM
To: matthew@goldsteinpllc.com

KW

Matt,

You requested DOPSR respond NLT the end of the year on these issues in your 2 Dec e-mail.

I've attached three letters, the first clarifying case 15-S-2473 (only the printed or rendered images not the actual CAD files are cleared for public release), a copy of the original approval letter for that case, and the outcomes of 15-S-0358 and 15-S-0514 (again only the printed or rendered images are cleared for public release). Please see the letters for additional explanation.

I've been short staffed this holiday period and regret not sending them to you previously. Hard copies will also be sent regular mail.

R,

Wally King, P.E.
Chief, Technology Branch
Defense Office of Prepublication and Security Review
Department of Defense
Room 2A534, The Pentagon
Direct line: 703-614-4908
General line: 703-614-5001
<http://www.dtic.mil/whs/esd/osr/>

-----Original Message-----

From: matthew@goldsteinpllc.com [mailto:matthew@goldsteinpllc.com]
Sent: Wednesday, December 10, 2014 7:20 AM
To: King, Walter J CIV WHS ESD (US)
Subject: RE: Meeting re Open Defense Distributed Requests

Wally,

Files for the Collapsible stock receiver is attached.

-Matt

Matthew A. Goldstein | Counsel
1012 14th Street, NW, Suite 620
Washington, DC 20005
C: 1.202.550.0040
www.GoldsteinPLLC.com

This message may contain information that is privileged and/or confidential. As such, it is solely intended for disclosure to the recipient named above. Access by anyone other than the intended recipient is unauthorized. If you have received this electronic transmission in error, please immediately reply that you have received the message and delete the message. Note that if you are not the intended recipient, any copying, disclosure, distribution, or other unauthorized use of the information contained in this message is prohibited and may be unlawful. Thank you.

----- Original Message -----

Subject: RE: Meeting re Open Defense Distributed Requests
From: "King, Walter J CIV WHS ESD (US)" <walter.j.king.civ@mail.mil>
Date: 12/9/14 1:30 pm
To: "Matthew Goldstein" <matthew@goldsteinpllc.com>

Matt,

While you forwarded the 9 Oct letter a couple of times, I don't think the attachments made it to us. I can't find any evidence it was actually delivered to our SECREV account. Perhaps it was sent on the day we exceeded our storage allocation?

Unlike the 23 Oct letter which had e-mail attachments when sent to our SECREV office e-mail account--so we could process that request even though the FedEx it referenced was returned to your client and not delivered.

R,

Wally

-----Original Message-----

From: Matthew Goldstein [mailto:matthew@goldsteinpllc.com]
Sent: Wednesday, December 03, 2014 11:33 AM
To: King, Walter J CIV WHS ESD (US)
Cc: Kluzik, Donald E CIV WHS ESD (US)
Subject: Re: Meeting re Open Defense Distributed Requests
Importance: High

Thanks Wally.

The October 9 and 23 requests are for electronic files and images that pertain to two different AR-15 lower receiver variants (one is "metal" and the other is for "collapsible stock").

Were both requests consolidated and assigned re same case no (i.e., 15-S-0358)?

-Matt

Matthew A. Goldstein | Counsel
1012 14th Street, NW, Suite 620
Washington, DC 20005
C: +1.202.550.0040

> On Dec 3, 2014, at 9:37 AM, King, Walter J CIV WHS ESD (US) <walter.j.king.civ@mail.mil> wrote:

>

> Mr. Goldstein,

>

> This request was assigned case number 15-S-0358 (Mr. Don Kluzik is my AO), this case was assigned for review outside our organization, and is due back 5 Dec 2014. I know of no delays, but we don't consider the case late until the due date has passed.

>

> I'll contact the reviewing office next Monday if we don't get their response this week.

>

> While Tina assisted both of us in tracking down delivery difficulties she doesn't normally work security review cases. She is our dedicated security manager. It's ok to exclude her in future correspondence. You're welcome to contact myself or Mr. Kluzik for future updates.

>

> R,

>

> Wally

>

>

>

> -----Original Message-----

> From: Matthew Goldstein [mailto:matthew@goldsteinpllc.com]

> Sent: Tuesday, December 02, 2014 2:14 PM

> To: King, Walter J CIV WHS ESD (US); Riley, Tina L CIV WHS ESD (US)

> Subject: Re: Meeting re Open Defense Distributed Requests

>

> Hit send too soon - requests are attached to this email.

>

> Thanks.

>

> -Matt

>

>

>

>> On Dec 2, 2014, at 2:12 PM, Matthew Goldstein <matthew@goldsteinpllc.com> wrote:

>>

>> Wally and Tina,

>>

>> Just checking in on status of the attached October Defense Distributed requests for OSR review/clearance.

>>

>> We'd like to get responses for the company by the end of the year. I'd like to visit with you in-person to informally discuss and perhaps answer any questions you may have if there's something in particular holding up the reviews.

>>

>> Are you available to meet Monday 12/8 at 11:00 am?

>>

>> Thanks.

>>

>> -Matt

>>

>>

>> Matthew A. Goldstein | Counsel

>> 1012 14th Street, NW, Suite 620

>> Washington, DC 20005

>> ~~~~~

>> C: +1.202.550.0040
>> www.GoldsteinPLLC.com
>>

>> This message may contain information that is privileged and/or confidential. As such, it is solely intended for disclosure to the recipient named above. Access by anyone other than the intended recipient is unauthorized. If you have received this electronic transmission in error, please immediately reply that you have received the message and delete the message. Note that if you are not the intended recipient, any copying, disclosure, distribution, or other unauthorized use of the information contained in this message is prohibited and may be unlawful. Thank you.

>>
>>
>>
>>
>
>



14-S-2473 (clarification)
14-S-2473 ...d 0514.pdf



DEPARTMENT OF DEFENSE
 DEFENSE OFFICE OF PREPUBLICATION AND SECURITY REVIEW
 1155 DEFENSE PENTAGON
 WASHINGTON, DC 20301-1155

December 22, 2014
 Ref: 14-S-2473

Mr. Cody R. Wilson
 Defense Distributed
 1101 West 34th Street, #340
 Austin, TX 78705

Dear Mr. Wilson:

This is a clarification to the enclosed September 25, 2014, correspondence providing public release approval of the indicated documents titled:

- “AR-15 Lower Receiver”

The Defense Office of Prepublication and Security Review (DOPSR) desires to clarify the previous approval for public release was in compliance with the International Traffic in Arms Regulations (ITAR) 125.4(b)(13) including ITAR 125.4(a) which states this exemption “are also not applicable for purposes of establishing offshore procurement arrangements *or producing defense articles offshore...*”

In other words, only the **rendered images** previously requested for review (hard copy or electronic) included within the subject request are **APPROVED** for public release as previously stated in our 25 September letter, *however, to clarify*, public release approval of **the actual electronic CAD files** your request letter states “can be used with a 3D printer or a computer numerical control machine to *produce* the hardware depicted in the rendered images of the electronic files” cannot be approved under ITAR 125.4(b)(13), DOPSR’s sole ITAR mention, and **are therefore beyond the purview of DOPSR.**

DOPSR recommends you contact the Department of State, Bureau of Political Military Affairs, Office of Defense Trade Controls Compliance regarding public release of any electronic CAD files that can assist in *producing* defense articles controlled under the ITAR.

Please direct any questions regarding this case to Mr. Donald Kluzik at 703-614-4931, email: donald.e.kluzik.civ@mail.mil.

Sincerely,


 M. M. Langerman
 Chief

Enclosures:
 As stated

September 25, 2014
Ref: 14-S-2473

Mr. Cody R. Wilson
Defense Distributed
1101 West 34th Street, #340
Austin, TX 78705

Dear Mr. Wilson:

This is in response to the enclosed September 2, 2014, correspondence requesting public release approval of the enclosed documents titled:

- “AR-15 Lower Receiver”

The documents are **APPROVED** for public release. However, this approval does not include any photograph, picture, exhibit, caption, or other supplemental material not specifically approved by this office. Our concurrence for release does not imply DoD endorsement or factual accuracy of the material.

Please direct any questions regarding this case to Mr. Donald Kluzik at 703-614-4931, email: donald.e.kluzik.civ@mail.mil.

Sincerely,



)
M. M. Langerman
Chief

Enclosures:
As stated

Prepared by: dekluzik:9/25/14:DOPSR:703-614-4931:gr DK pk _____



DEPARTMENT OF DEFENSE
 DEFENSE OFFICE OF PREPUBLICATION AND SECURITY REVIEW
 1155 DEFENSE PENTAGON
 WASHINGTON, DC 20301-1155

December 22, 2014
 Ref: 15-S-0358
 15-S-0514

Mr. Cody R. Wilson
 Defense Distributed
 1101 West 34th Street, #340
 Austin, TX 78705

Dear Mr. Wilson:

This is in response to the letters requesting public release approval of the indicated documents titled:

- “AR-15 Lower Receiver (C)”
- “AR-15 Lower Receiver (M)”

The Defense Office of Prepublication and Security Review (DOPSR) must stay consistent with previous approvals for public release and in compliance with the International Traffic in Arms Regulations (ITAR) 125.4(b)(13) including ITAR 125.4(a) which states this exemption “are also not applicable for purposes of establishing offshore procurement arrangements *or producing defense articles offshore...*”

Therefore, only the **rendered images** requested for review (hard copy or electronic) included within the subject request are **APPROVED** for public release. Public release approval of **the actual electronic CAD files** your request letter states “can be used with a 3D printer or a computer numerical control machine to *produce* the hardware depicted in the rendered images of the electronic files” cannot be approved under ITAR 125.4(b)(13), DOPSR’s sole ITAR mention, and **are therefore beyond the purview of DOPSR.**

DOPSR recommends you contact the Department of State, Bureau of Political Military Affairs, Office of Defense Trade Controls Compliance regarding public release of any electronic CAD files that can assist in *producing* defense articles controlled under the ITAR.

Please direct any questions regarding this case to Mr. Donald Kluzik at 703-614-4931, email: donald.e.kluzik.civ@mail.mil.

Sincerely,


 M. M. Langerman
 Chief

Enclosures:
 As stated

EXHIBIT 23

MATTHEW A. GOLDSTEIN, PLLC
INTERNATIONAL TRADE
1012 14TH STREET, NW, SUITE 620
WASHINGTON, D.C. 20005

BY COURIER / FEDERAL EXPRESS

Advanced Copy by Email to DDTCResponseTeam@state.gov

January 5, 2015

Ed Peartree, Director
Office of Defense Trade Controls Policy
U.S. Department of State
PM/DDTC, SA-1, 12th Floor
2401 E Street, NW
Washington, D.C. 20037

SUBJECT: Advisory Opinion Request How to Obtain Prepublication Approval of CAD Files from DDTC Compliance and/or Other Agencies/DDTC Divisions
Defense Distributed, Inc., PM/DDTC Code M-34702

Dear Mr. Peartree:

Pursuant to Section 126.9 and 129.10 of the International Traffic in Arms Regulations ("ITAR") (22 C.F.R. Sections 120-130), Defense Distributed requests an advisory opinion from the Directorate of Defense Trade Controls ("DDTC") on how to obtain prepublication approval from the Office of Defense Trade Controls Compliance ("DDTC Compliance") to transmit privately generated unclassified Computer Assisted Drawing ("CAD") files into the Internet and other public forums.

The request also seeks DDTC advisement on what kinds of software, CAD, and other electronic files are reviewable by the Department of Defense Department Office of Prepublication and Security Review ("DOPSR") for public release.

A copy of recent letters from DOPSR recommending that Defense Distributed pursue prepublication approval with DDTC Compliance for public postings of CAD files is provided with this request at Attachment 1.

A letter from Defense Distributed authorizing my law firm to file this request is enclosed at Attachment 2. Please direct any questions and all correspondence related to this request to my office. Communications to me at matthew@goldsteinpllc.com are preferred.

I. BACKGROUND

Defense Distributed is a Texas corporation, registered with the Department of State as a defense article manufacturer under PM/DDTC Code M-34702. The company has developed technical information that can be used to produce, manufacture, and assemble various parts components, accessories, and attachments to firearms that may be controlled under the ITAR.

Internet Publications Advisory Opinion Request
January 5, 2015
Page 2 of 3

Following notification from DDTC in May 8, 2013, that the agency requires U.S. Government prior approval before publications of technical information into the public forums (Attachment 3), Defense Distributed has submitted requests for U.S. Government clearance of technical data on Defense Distributed projects to DOPSR.¹

On September 2, 2014, Defense Distributed sent DOPSR a request for prepublication approval for public release of certain CAD files. DOPSR assigned the request case no. 14-S-2473.

On October 9, 2014, Defense Distributed sent DOPSR two additional requests for prepublication approval for public release of certain CAD files. DOPSR assigned the requests case nos. 15-S-0358 and 15-S-0514.

Copies of the letters sent with Defense Distributed requests to DOPSR are provided at Attachment 4.

On December 31, 2014, DOPSR sent Plaintiff two letters (Attachment 1), postdated December 22, 2014, responding to the Defense Distributed CAD file release requests. The DOPSR letters state that DOPSR will not review the CAD files because the files can be used to “produce” defense articles and can be used in “offshore procurement.” In the letters, DOPSR further states:

DOPSR recommends you contact the Department of State, Bureau of Political Military Affairs, Office of Defense Trade Controls Compliance regarding public release of any electronic CAD files that can assist in *producing* defense articles controlled under the ITAR.

II. SPECIFIC REQUEST FOR GUIDANCE

Defense Distributed requests DDTC guidance on the following specific questions:

1. What is the specific process for obtaining prepublication approval from DDTC Compliance to transmit privately generated unclassified CAD files, and other files into the Internet and other public forums?
2. What kinds of software, CAD, and other electronic files are reviewable by DOPSR for public release?
3. What kinds of software, CAD, and other electronic files are reviewable by DDTC Compliance for public release?

¹ In complying with current DDTC-imposed restrictions on publication of technical information into the public domain, Defense Distributed does not intent to, nor should it be considered to, waive any defense, claim or right under law.

Internet Publications Advisory Opinion Request
January 5, 2015
Page 3 of 3

4. What kinds of software, CAD, and other electronic files are reviewable by other DDTC Divisions for public release?

III. REQUEST FOR EXPEDITED CONSIDERATION

Defense Distributed understands that DDTC normally responds to advisory opinion requests in thirty (30) days. However, time is of the essence when speech restrained by a government agency. Accordingly, please advise if DDTC will require more than thirty (30) days to answer this request so that the Defense Distributed can plan accordingly.

Thank you for your prompt attention to this matter and please contact me at 202-550-0040 or at matthew@goldsteinpllc.com if any additional information is needed.

Yours truly,



Matthew A. Goldstein
Legal Counsel

ENCLOSURES:

Original and Seven (7) Copies of this Request

- | | |
|--------------|---|
| Attachment 1 | Department of Defense December 22, 2015 Letter |
| Attachment 2 | Letter Authorizing Counsel to File Advisory Opinion Request |
| Attachment 3 | May 8, 2013 DDTC Letter to Defense Distributed |
| Attachment 4 | Defense Distributed Letters Accompanying Subject DOPSR Requests |

ATTACHMENT 1



DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF PREPUBLICATION AND SECURITY REVIEW
1155 DEFENSE PENTAGON
WASHINGTON, DC 20301-1155

December 22, 2014
Ref: 14-S-2473

Mr. Cody R. Wilson
Defense Distributed
1101 West 34th Street, #340
Austin, TX 78705

Dear Mr. Wilson:

This is a clarification to the enclosed September 25, 2014, correspondence providing public release approval of the indicated documents titled:

- "AR-15 Lower Receiver"

The Defense Office of Prepublication and Security Review (DOPSR) desires to clarify the previous approval for public release was in compliance with the International Traffic in Arms Regulations (ITAR) 125.4(b)(13) including ITAR 125.4(a) which states this exemption "are also not applicable for purposes of establishing offshore procurement arrangements *or producing defense articles offshore...*"

In other words, only the **rendered images** previously requested for review (hard copy or electronic) included within the subject request are **APPROVED** for public release as previously stated in our 25 September letter, *however, to clarify*, public release approval of **the actual electronic CAD files** your request letter states "can be used with a 3D printer or a computer numerical control machine to *produce* the hardware depicted in the rendered images of the electronic files" cannot be approved under ITAR 125.4(b)(13), DOPSR's sole ITAR mention, and **are therefore beyond the purview of DOPSR.**

DOPSR recommends you contact the Department of State, Bureau of Political Military Affairs, Office of Defense Trade Controls Compliance regarding public release of any electronic CAD files that can assist in *producing* defense articles controlled under the ITAR.

Please direct any questions regarding this case to Mr. Donald Kluzik at 703-614-4931, email: donald.e.kluzik.civ@mail.mil.

Sincerely,


M. M. Langerman
Chief

Enclosures:
As stated

September 25, 2014
Ref: 14-S-2473

Mr. Cody R. Wilson
Defense Distributed
1101 West 34th Street, #340
Austin, TX 78705

Dear Mr. Wilson:

This is in response to the enclosed September 2, 2014, correspondence requesting public release approval of the enclosed documents titled:

- “AR-15 Lower Receiver”

The documents are **APPROVED** for public release. However, this approval does not include any photograph, picture, exhibit, caption, or other supplemental material not specifically approved by this office. Our concurrence for release does not imply DoD endorsement or factual accuracy of the material.

Please direct any questions regarding this case to Mr. Donald Kluzik at 703-614-4931, email: donald.e.kluzik.civ@mail.mil.

Sincerely,



)
M. M. Langerman
Chief

Enclosures:
As stated

Prepared by: dekluzik:9/25/14:DOPSR:703-614-4931:gr DK pk _____



DEPARTMENT OF DEFENSE
 DEFENSE OFFICE OF PREPUBLICATION AND SECURITY REVIEW
 1155 DEFENSE PENTAGON
 WASHINGTON, DC 20301-1155

December 22, 2014

Ref: 15-S-0358

15-S-0514

Mr. Cody R. Wilson
 Defense Distributed
 1101 West 34th Street, #340
 Austin, TX 78705

Dear Mr. Wilson:

This is in response to the letters requesting public release approval of the indicated documents titled:

- "AR-15 Lower Receiver (C)"
- "AR-15 Lower Receiver (M)"

The Defense Office of Prepublication and Security Review (DOPSR) must stay consistent with previous approvals for public release and in compliance with the International Traffic in Arms Regulations (ITAR) 125.4(b)(13) including ITAR 125.4(a) which states this exemption "are also not applicable for purposes of establishing offshore procurement arrangements *or producing defense articles offshore...*"

Therefore, only the **rendered images** requested for review (hard copy or electronic) included within the subject request are **APPROVED** for public release. Public release approval of **the actual electronic CAD files** your request letter states "can be used with a 3D printer or a computer numerical control machine to *produce* the hardware depicted in the rendered images of the electronic files" cannot be approved under ITAR 125.4(b)(13), DOPSR's sole ITAR mention, and **are therefore beyond the purview of DOPSR.**

DOPSR recommends you contact the Department of State, Bureau of Political Military Affairs, Office of Defense Trade Controls Compliance regarding public release of any electronic CAD files that can assist in *producing* defense articles controlled under the ITAR.

Please direct any questions regarding this case to Mr. Donald Kluzik at 703-614-4931, email: donald.e.kluzik.civ@mail.mil.

Sincerely,

for 
 M. M. Langerman
 Chief

Enclosures:
 As stated

ATTACHMENT 2



BY COURIER / FEDERAL EXPRESS

Advanced Copy by Email to DDTCResponseTeam@state.gov

January 5, 2015

Ed Peartree, Director
Office of Defense Trade Controls Policy
U.S. Department of State
PM/DDTC, SA-1, 12th Floor
2401 E Street, NW
Washington, D.C. 20037

SUBJECT: Letter authorizing Matthew A. Goldstein, PLLC to submit Advisory Opinion Request on behalf of Defense Distributed

Dear Sir or Madam:

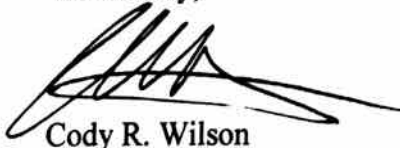
The Law Office of Matthew A. Goldstein, PLLC is authorized to submit an Advisory Opinion request to the Directorate of Defense Trade Controls ("DDTC") on behalf of Defense Distributed, Inc. for advisement on how to obtain prepublication approval from the Office of Defense Trade Controls Compliance ("DDTC Compliance") to transmit privately generated unclassified Computer Assisted Drawing ("CAD") files into the Internet and other public forums; and on what kinds of software, CAD, and other electronic files are reviewable by the Department of Defense Department Office of Prepublication and Security Review for public release.

Defense Distributed authorizes DDTC personnel and other U.S. Government representatives to speak with and to release information pertaining to the request to Mr. Goldstein, who can be reached at:

Matthew A. Goldstein
1012 14th Street, NW, Suite 620
Washington, DC 20005
(202) 550-0040
matthew@goldsteinpllc.com

Thank you in advance for your consideration.

Yours truly,



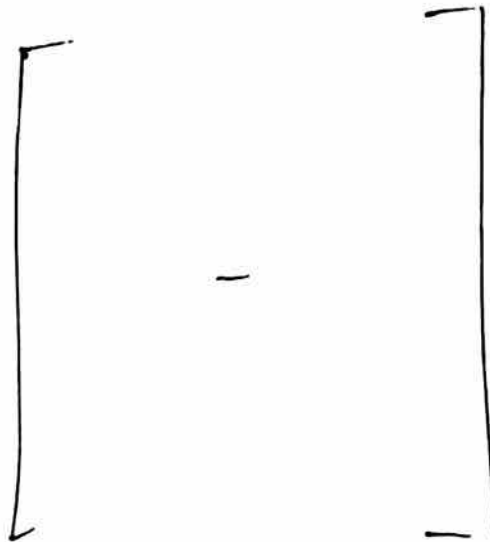
Cody R. Wilson

DefDist | 1101 W 34th St. # 340 Austin, TX 78705 | DefDist.org

Office of Security Review
Page 1 of 2



Principal, Defense Distributed, Inc.
1101 W 34th St. #340
Austin, Texas 78705
(501) 743-9680
crw@defcad.com



ATTACHMENT 3



United States Department of State
Bureau of Political-Military Affairs
Office of Defense Trade Controls Compliance
Washington, D.C. 20522-0112

MAY 08 2013

In reply refer to
[REDACTED]

Mr. Cody Wilson
Defense Distributed
[REDACTED]

Dear Mr. Wilson:

The Department of State, Bureau of Political Military Affairs, Office of Defense Trade Controls Compliance, Enforcement Division (DTCC/END) is responsible for compliance with and civil enforcement of the Arms Export Control Act (22 U.S.C. 2778) (AECA) and the AECA's implementing regulations, the International Traffic in Arms Regulations (22 C.F.R. Parts 120-130) (ITAR). The AECA and the ITAR impose certain requirements and restrictions on the transfer of, and access to, controlled defense articles and related technical data designated by the United States Munitions List (USML) (22 C.F.R. Part 121).

DTCC/END is conducting a review of technical data made publicly available by Defense Distributed through its 3D printing website, DEF CAD.org, the majority of which appear to be related to items in Category I of the USML. Defense Distributed may have released ITAR-controlled technical data without the required prior authorization from the Directorate of Defense Trade Controls (DDTC), a violation of the ITAR.

Technical data regulated under the ITAR refers to information required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance or modification of defense articles, including information in the form of blueprints, drawings, photographs, plans, instructions or documentation. For a complete definition of technical data, see § 120.10 of the ITAR. Pursuant to § 127.1 of the ITAR,

it is unlawful to export any defense article or technical data for which a license or written approval is required without first obtaining the required authorization from the DDTC. Please note that disclosing (including oral or visual disclosure) or transferring technical data to a foreign person, whether in the United States or abroad, is considered an export under § 120.17 of the ITAR.

The Department believes Defense Distributed may not have established the proper jurisdiction of the subject technical data. To resolve this matter officially, we request that Defense Distributed submit Commodity Jurisdiction (CJ) determination requests for the following selection of data files available on DEFCAD.org, and any other technical data for which Defense Distributed is unable to determine proper jurisdiction:

1. Defense Distributed Liberator pistol
2. .22 electric
3. 125mm BK-14M high-explosive anti-tank warhead
4. 5.56/.223 muzzle brake
5. Springfield XD-40 tactical slide assembly
6. Sound Moderator – slip on
7. “The Dirty Diane” 1/2-28 to 3/4-16 STP S3600 oil filter silencer adapter
8. 12 gauge to .22 CB sub-caliber insert
9. Voltlock electronic black powder system
10. VZ-58 front sight.

DTCC/END requests that Defense Distributed submit its CJ requests within three weeks of receipt of this letter and notify this office of the final CJ determinations. All CJ requests must be submitted electronically through an online application using the DS-4076 Commodity Jurisdiction Request Form. The form, guidance for submitting CJ requests, and other relevant information such as a copy of the ITAR can be found on DDTC’s website at <http://www.pmddtc.state.gov>.

Until the Department provides Defense Distributed with final CJ determinations, Defense Distributed should treat the above technical data as ITAR-controlled. This means that all such data should be removed from public access immediately. Defense Distributed should also review the remainder of the data made public on its website to

- 3 -

determine whether any additional data may be similarly controlled and proceed according to ITAR requirements.

Additionally, DTCC/END requests information about the procedures Defense Distributed follows to determine the classification of its technical data, to include the aforementioned technical data files. We ask that you provide your procedures for determining proper jurisdiction of technical data within 30 days of the date of this letter to Ms. Bridget Van Buren, Compliance Specialist, Enforcement Division, at the address below:

Office of Defense Trade Controls Compliance
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

We appreciate your full cooperation in this matter. Please note our reference number in any future correspondence.

Sincerely,



Glenn E. Smith
Chief, Enforcement Division

ATTACHMENT 4



BY FEDERAL EXPRESS

ADVANCE COPY BY ELECTRONIC MAIL

(whs.pentagon.esd.mbx.secrev@mail.mil)

September 2, 2014

Department of Defense
Office of Security Review
2A534, Pentagon
Washington DC 20301-1155

Subject: Request for OSR Review of AR-15 Lower Receiver Documents

Dear Department Representative:

This is a request for review under ITAR Section 125.4(b)(13) and DoDD 5230.29.

Accompanying this letter please find the documents for review. They consist of two (2) electronic files (.STP, and .STL formats) for a lower receiver to the AR-15 rifle and five (5) rendered images of the electronic files. These documents are also attached to the email transmitting and advance copy of this letter.

The original of this letter, five (5) CD-ROMs containing the electronic files, and five (5) unbound copies of the rendered images for review, are being sent contemporaneously herewith by Federal Express.

The electronic files are Computer Assisted Drafting ("CAD") files that can be used with a 3D printer or a computer numerical control machine to produce the hardware depicted in the rendered images of the electronic files.

These documents were created by John Sullivan, who is an employee of Defense Distributed. Defense Distributed is a Texas corporation. It is registered with the Department of State as a Defense Article Manufacturer under registration number M-34702.

The information contained in the documents is NOT company proprietary, was NOT developed under any U.S. Government contract, and is NOT subject to any government contract restrictions on dissemination.

These documents are NOT in the public domain. However, public release of the information contained in documents will not harm national security because design

DefDist | 1101 W 34th St. # 340 Austin, TX 78705 | DefDist.org

Office of Security Review
Page 1 of 3



specifications containing similar information and similar CAD files for AR-15 lower receivers are already publicly available online.

.STP and/or .STL files for AR-15 lower receivers are already publicly available for download at a variety of web addresses, to include the following:

www.3dcadbrowser.com/download.aspx?3dmodel=42013
<http://grabcad.com/library/ar-15-lower-receiver>
<http://grabcad.com/library/a-printable-ar15-lower-receiver>
<https://grabcad.com/library/ar15-lower-concept-1>
<http://grabcad.com/library/ar-15-lower-receiver>

Other CAD file formats for lower receivers to the AR-15 are also publicly available online at web addresses, to include the following:

www.3dcadbrowser.com/download.aspx?3dmodel=42013
www.cncguns.com/downloads.html

In addition, detailed design specifications for AR-15 lower receivers are also available online from a variety of sources, to include the following:

www.homegunsmith.com/archive/T6215.html
www.ar15.com/archive/topic.html?b=3&f=4&t=619878
www.advancedrifles.com/build-it-yourself
www.biggerhammer.net/ar15/cad/

I expect to publish the documents on the Defense Distributed website on or about October 1, 2014. OSR review of the documents is therefore needed before September 30, 2014, but review after this time is acceptable in lieu of return without action.

Response by email to me at crw@defdist.org is preferred. If mailing the response, the address for mailing is: 1101 West 34th St., #340, Austin, Texas 78705.

Thank you for your consideration in the matter. I can be reached at (501) 743-9680 with any questions, comments or concerns.

Sincerely,

A handwritten signature in black ink, appearing to read "Cody R. Wilson", with a long horizontal flourish extending to the right.

Cody R. Wilson
Director
Defense Distributed, Inc.



Att./Encl.:

.IPT Electronic File for AR-15 Lower Receiver (CD-ROM)
.STEP Electronic File for AR-15 Lower Receiver (CD-ROM)
.STL Electronic File for AR-15 Lower Receiver (CD-ROM)
5 Rendered Images of .STEP and .STL files

]

]



BY FEDERAL EXPRESS

ADVANCE COPY BY ELECTRONIC MAIL

(whs.pentagon.esd.mbx.secrev@mail.mil)

October 9, 2014

Department of Defense
Office of Security Review
2A534, Pentagon
Washington DC 20301-1155

Subject: Request for OSR Review of AR-15 Lower Receiver Documents (M)

Dear Department Representative:

This is a request for review under ITAR Section 125.4(b)(13) and DoDD 5230.29.

Accompanying this letter please find the documents for review. They consist of two (2) electronic files (.STP, and .STL formats) for a lower receiver to the AR-15 rifle and five (5) rendered images of the electronic files. These documents are also attached to the email transmitting and this advance copy letter.

The original of this letter, five (5) CD-ROMs containing the electronic files, and five (5) unbound copies of the rendered images for review, are being sent contemporaneously herewith by Federal Express.

The electronic files are Computer Assisted Drafting ("CAD") files that can be used with a 3D printer or a computer numerical control machine to produce the hardware depicted in the rendered images of the electronic files.

These documents were created by John Sullivan, who is an employee of Defense Distributed. Defense Distributed is a Texas corporation. It is registered with the Department of State as a Defense Article Manufacturer under registration number M-34702.

The information contained in the documents is NOT company proprietary, was NOT developed under any U.S. Government contract, and is NOT subject to any government contract restrictions on dissemination.

These documents are NOT in the public domain. However, public release of the information contained in documents will not harm national security because design

DefDist | 1101 W 34th St. # 340 Austin, TX 78705 | DefDist.org

Office of Security Review
Page 1 of 3



specifications containing similar information and similar CAD files for AR-15 lower receivers are already publicly available online.

.STP and/or .STL files for AR-15 lower receivers are already publicly available for download at a variety of web addresses, to include the following:

www.3dcadbrowser.com/download.aspx?3dmodel=42013
<http://grabcad.com/library/ar-15-lower-receiver>
<http://grabcad.com/library/a-printable-ar15-lower-receiver>
<https://grabcad.com/library/ar15-lower-concept-1>
<http://grabcad.com/library/ar-15-lower-receiver>

Other CAD file formats for lower receivers to the AR-15 are also publicly available online at web addresses, to include the following:

www.3dcadbrowser.com/download.aspx?3dmodel=42013
www.cncguns.com/downloads.html

In addition, detailed design specifications for AR-15 lower receivers are also available online from a variety of sources, to include the following:

www.homegunsmith.com/archive/T6215.html
www.ar15.com/archive/topic.html?b=3&f=4&t=619878
www.advancedrifles.com/build-it-yourself
www.biggerhammer.net/ar15/cad/

I expect to publish the documents on the Defense Distributed website on or about October 1, 2014. OSR review of the documents is therefore needed before November 3, 2014, but review after this time is acceptable in lieu of return without action.

Response by email to me at crw@defdist.org is preferred. If mailing the response, the address for mailing is: 1101 West 34th St., #340, Austin, Texas 78705.

Thank you for your consideration in the matter. I can be reached at (501) 743-9680 with any questions, comments or concerns.

Sincerely,

A handwritten signature in black ink, appearing to read "Cody R. Wilson", with a stylized flourish extending to the right.

Cody R. Wilson
Director
Defense Distributed, Inc.



Att./Encl.:

.STP Electronic File for AR-15 Lower Receiver (Metal) (CD-ROM)
.STL Electronic File for AR-15 Lower Receiver (Metal) (CD-ROM)
5 Rendered Images of .STP and .STL files





BY FEDERAL EXPRESS

ADVANCE COPY BY ELECTRONIC MAIL

(whs.pentagon.esd.mbx.secrev@mail.mil)

October 9, 2014

Department of Defense
Office of Security Review
2A534, Pentagon
Washington DC 20301-1155

Subject: Request for OSR Review of AR-15 Lower Receiver Documents (C)

Dear Department Representative:

This is a request for review under ITAR Section 125.4(b)(13) and DoDD 5230.29.

Accompanying this letter please find the documents for review. They consist of two (2) electronic files (.STP, and .STL formats) for a lower receiver to the AR-15 rifle and five (5) rendered images of the electronic files. These documents are also attached to the email transmitting and this advance copy letter.

The original of this letter, five (5) CD-ROMs containing the electronic files, and five (5) unbound copies of the rendered images for review, are being sent contemporaneously herewith by Federal Express.

The electronic files are Computer Assisted Drafting ("CAD") files that can be used with a 3D printer or a computer numerical control machine to produce the hardware depicted in the rendered images of the electronic files.

These documents were created by John Sullivan, who is an employee of Defense Distributed. Defense Distributed is a Texas corporation. It is registered with the Department of State as a Defense Article Manufacturer under registration number M-34702.

The information contained in the documents is NOT company proprietary, was NOT developed under any U.S. Government contract, and is NOT subject to any government contract restrictions on dissemination.

These documents are NOT in the public domain. However, public release of the information contained in documents will not harm national security because design

DefDist | 1101 W 34th St. # 340 Austin, TX 78705 | DefDist.org

Office of Security Review
Page 1 of 3



specifications containing similar information and similar CAD files for AR-15 lower receivers are already publicly available online.

.STP and/or .STL files for AR-15 lower receivers are already publicly available for download at a variety of web addresses, to include the following:

www.3dcadbrowser.com/download.aspx?3dmodel=42013
<http://grabcad.com/library/ar-15-lower-receiver>
<http://grabcad.com/library/a-printable-ar15-lower-receiver>
<https://grabcad.com/library/ar15-lower-concept-1>
<http://grabcad.com/library/ar-15-lower-receiver>

Other CAD file formats for lower receivers to the AR-15 are also publicly available online at web addresses, to include the following:

www.3dcadbrowser.com/download.aspx?3dmodel=42013
www.cncguns.com/downloads.html

In addition, detailed design specifications for AR-15 lower receivers are also available online from a variety of sources, to include the following:

www.homegunsmith.com/archive/T6215.html
www.ar15.com/archive/topic.html?b=3&f=4&t=619878
www.advancedrifles.com/build-it-yourself
www.biggerhammer.net/ar15/cad/

I expect to publish the documents on the Defense Distributed website on or about October 1, 2014. OSR review of the documents is therefore needed before November 3, 2014, but review after this time is acceptable in lieu of return without action.

Response by email to me at crw@defdist.org is preferred. If mailing the response, the address for mailing is: 1101 West 34th St., #340, Austin, Texas 78705.

Thank you for your consideration in the matter. I can be reached at (501) 743-9680 with any questions, comments or concerns.

Sincerely,

Cody R. Wilson
Director
Defense Distributed, Inc.



Att./Encl.:

.STP Electronic File for AR-15 Lower Receiver (Collapsible Stock) (CD-ROM)
.STL Electronic File for AR-15 Lower Receiver (Collapsible Stock) (CD-ROM)
5 Rendered Images of .STP and .STL files

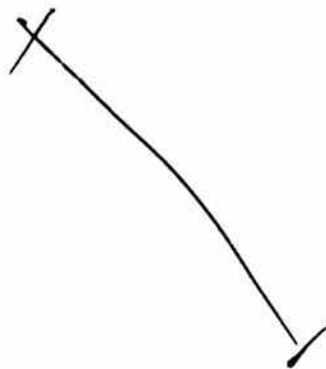


EXHIBIT 5

Directorate of Defense Trade Controls

Announcements Archives: 2014

Archives by Year: [2015](#) | [2013](#) | [2012](#) | [2011](#) | [2010](#) | [2009](#) | [2008](#) | [2007](#)

Dec | Nov | [Oct](#) | [Sep](#) | [Aug](#) | [Jul](#) | [Jun](#) | [May](#) | [Apr](#) | [Mar](#) | [Feb](#) | [Jan](#)

December

- **Federal Register Notice:** Notice of Temporary modification of Category XI of the United States Munitions List (12.30.14)
[Click here to read](#)
- **Industry Notice:** In support of Federal Register Notices [79 FR 37536](#) and [79 FR 66608](#), DTrade DSP forms (i.e., DSP-5, -61, and -73), DSP-85 (a fillable PDF form), and the Common Schema have been upgraded to accommodate the additions and revisions to USML Categories VIII, XI, XV and XIX. Beginning **December 30, 2014**, DTrade users must use version 8.5 for the DSP-5 and -61, version 8.6 for the DSP-73, version 3.0 for the DSP-85, and version 7.4 for the Common Schema to submit license applications. Earlier versions of these forms and schema will automatically be rejected by the system beginning on **December 30, 2014**. To access the new DTrade forms and Common Schema, [click here](#). To access the new DSP-85, [click here](#). (12.30.14)
- **Licensing:** Effective December 30, 2014, DDTC will make a slight change to the DTrade submission requirements for certain subparagraphs within USML Category XI. [Click here to read](#). (12.29.14)
- **Web Notice:** Two (2) new Name/Address change announcements have been posted. (12.04.14)
[Click here to read](#).

November

- **Industry Notice:** Pursuant to §126.3 of the ITAR and only for the export of Government Furnished Equipment hand carried out of the United States for use in service of a U.S. government contract, the Deputy Assistant Secretary for Defense Trade Controls has waived the provision in §123.22(a)(2) which requires Customs and Border Protection (CBP) to decrement DSP-73 temporary export licenses under certain circumstances. [Click here](#) for further information. [FAQs](#) are also available. (11.26.14)
- **Federal Register Notice:** Amendment to the International Traffic in Arms Regulations: Policy on Exports to Vietnam (11.17.14) [Click here to read](#)
- **Industry Notice:** Export Control Reform: The Export Control Reform (ECR) FAQs have been updated. [click here](#). (11.13.14)
- **Web Notice:** One (1) new Name/Address change announcements have been posted. (11.12.14)
[Click here to read](#).
- **Web Notice:** Three (3) new Name/Address change announcements have been posted. (11.05.14)
[Click here to read](#).
- **Web Notice:** One (1) new Name/Address change announcement has been posted. (11.04.14)
[Click here to read](#).

October

- **Federal Register Notice:** Amendment to the International Traffic in Arms Regulations: Corrections, Clarifications, and Movement of Definitions (10.17.14) [Click here to read](#)
- **Web Notice:** One (1) new Name/Address change announcement has been posted. (10.29.14)
[Click here to read](#).
- **Web Notice:** Two (2) new Name/Address changes announcement have been posted. (10.24.14)
[Click here to read](#).
- **Web Notice:** Three (3) new Name/Address changes announcement have been posted. (10.20.14)
[Click here to read](#).
- **Web Notice:** One (1) new Name/Address change announcement has been posted. (10.16.14)
[Click here to read](#).
- **Web Notice:** One (1) new Name/Address change announcement has been posted. (10.15.14)
[Click here to read](#).
- **Web Notice:** Two (2) new Name/Address changes announcement have been posted. (10.14.14)

[Click here to read.](#)

[Back to Top](#)

September

- **Web Notice:** One (1) new Name/Address change announcement has been posted. (09.29.14)
[Click here to read.](#)
- **Web Notice:** One (1) new Name/Address change announcement has been posted. (09.25.14)
[Click here to read.](#)
- **Web Notice:** One (1) acquisition announcement has been posted. (09.24.14)
[Click here to read.](#)
- **Web Notice:** Two (2) new Name/Address change announcements have been posted. (09.22.14)
[Click here to read.](#)
- **Web Notice:** One (1) new Name/Address change announcement has been posted. (09.18.14)
[Click here to read.](#)
- **Web Notice:** Four (4) new Name/Address change announcements have been posted. (09.15.14)
[Click here to read.](#)
- **Web Notice:** One (1) new Name/Address change announcement has been posted. (09.11.14)
[Click here to read.](#)
- **Web Notice:** One (1) new Name/Address change announcement has been posted. (09.05.14)
[Click here to read.](#)
- **Web Notice:** One (1) new Name/Address change announcement has been posted. (09.02.14)
[Click here to read.](#)

[Back to Top](#)

August

- **Web Notice:** One (1) new Name/Address change announcement has been posted. (08.28.14)
[Click here to read.](#)
- **Maintenance Notice:** The Directorate of Defense Trade Controls (DDTC) systems will undergo network maintenance on August 29, 2014 from 6:00pm until 10:00 pm EDT. During this time the DTrade system will be unavailable to accept submissions. The pmddtc.state.gov website will be unavailable as will EFS, TRS, ELLIE, and MARY. (08.28.14)
- **Web Notice:** Three (3) new Name/Address change announcements have been posted. (08.22.14)
[Click here to read.](#)
- **Web Notice:** One (1) new Name/Address change announcement has been posted. (08.20.14)
[Click here to read.](#)
- **Web Notice:** New Guideline/Instruction on 126.13 Requirements for Re-exports/Re-transfers under §123.9 has been posted. (08.20.14)
[Click here to read.](#)
- **Web Notice:** Five (5) new Name/Address change announcement have been posted. (08.12.14)
[Click here to read.](#)
- **Web Notice:** One (1) new Name/Address change announcement has been posted. (08.08.14)
[Click here to read.](#)
- **Web Notice:** Four (4) new Name/Address change announcement have been posted. (08.07.14)
[Click here to read.](#)

[Back to Top](#)

July

- **Web Notice:** One (1) new Name/Address change announcement has been posted. (07.28.14)
[Click here to read.](#)
- **Web Notice:** One (1) new Name/Address change announcement has been posted. (07.25.14)
[Click here to read.](#)
- **Web Notice:** One (1) new Name/Address change announcement has been posted. (07.23.14)

[Click here to read.](#)

- **Federal Register Notice:** Amendment to the International Traffic in Arms Regulations: United States Munitions List Category XI (Military Electronics), and Other Changes. (07.02.14)

[Click here to read.](#)

- **Compliance:** DTCC announces a correction to the publication of the Federal Register notice of administrative debarment of Carlos Dominguez, Elint, S.A., Spain Night Vision, S.A., SNV, S.A., and successor companies. (07.1.14)

[Click here to read.](#)

[Back to Top](#)

June

- **Industry Notice:** The Commodity Jurisdiction process is being impacted due to ongoing information technology assessments. Currently, CJs are being accepted for processing; however, companies submitting CJ requests should expect delays and plan accordingly. DDTC will advise once the assessments are completed. (06.03.14)
- **Industry Notice:** In support of Federal Register Notice 79 FR 34 and internal revisions, DTrade online forms, DS2032, and Common Schema have been updated. Effective July 1, 2014 earlier versions of these forms will not be accepted. (06.18.14)
[Click here to read.](#)
- **Federal Register Notice:** Amendment to the International Traffic in Arms Regulations: Third Rule Implementing Export Control Reform; Correction has been posted. (06.27.14)
[Click here to read.](#)
- **Licensing:** Revision 4.2 of the "Guidelines for Preparing Electronic Agreements" has been posted. (06.24.14)
[Click here to read.](#)
- **Web Notice:** One (1) new Name/Address change announcement has been posted. (06.24.14)
[Click here to read.](#)
- **Compliance:** DTCC announces the publication of the Federal Register notice of administrative debarment of Carlos Dominguez, Elint, S.A., Spain Night Vision, S.A., SNV, S.A., and successor companies. (06.20.14)
[Click here to read.](#)
- **Industry Notice:** In support of [Federal Register Notice 79 FR 34](#) and internal revisions, DTrade online forms, DS2032, and Common Schema have been updated. Effective July 1, 2014 earlier versions of these forms will not be accepted. (06.18.14)
- **Compliance:** Intersil Corporation administrative settlement has been posted. (06.18.14)
[Click here to read.](#)
- **Web Notice:** One (1) new Name/Address change announcement has been posted. (06.17.14)
[Click here to read.](#)
- **Web Notice:** One (1) new Name/Address change announcement has been posted. (06.16.14)
[Click here to read.](#)
- **Web Notice:** Four (4) new Name/Address change announcement has been posted. (06.12.14)
[Click here to read.](#)
- **Industry Notice:** The Department of State clarifies recent press release on tokenization and cloud computing.(06.11.14)
[Click here for more information](#)
- **Web Notice:** One (1) new Name/Address change announcement has been posted. (06.11.14)
[Click here to read.](#)
- **Compliance:** DTCC announces the administrative debarment of Carlos Dominguez, Elint, S.A., Spain Night Vision, S.A., SNV, S.A., and successor companies. This debarment is the result of the Department's first institution of an administrative proceeding against foreign persons by referral of a charging letter before an Administrative Law Judge. (06.05.14)
[Click here for more information](#)
- **Web Notice:** One (1) new Name/Address change announcement has been posted. (06.04.14)
[Click here to read.](#)
- **Industry Notice:** The Commodity Jurisdiction process is being impacted due to ongoing information technology assessments. Currently, CJs are being accepted for processing; however, companies submitting CJ requests should expect delays and plan accordingly. DDTC will advise once the assessments are completed. (06.03.14)

[Back to Top](#)

May

- **Web Notice:** Two (2) new Name/Address change announcement have been posted. (05.27.14)

[Click here to read.](#)

- **Web Notice:** One (1) new Name/Address change announcement has been posted. (05.23.14)
[Click here to read.](#)
- **Web Notice:** One (1) new Name/Address change announcement has been posted. (05.20.14)
[Click here to read.](#)
- **Press Release:** U.S. Department of State Publishes Changes to Regulations that Control Exports of Satellites and Related Items. (05.14.14)
[Click here to read the press release](#)
- **Web Notice:** One (1) new Name/Address change announcement has been posted. (05.13.14)
[Click here to read.](#)
- **Industry Notice:** The Department of State announced the expansion of export restrictions on Russia - April 28, 2014. (05.09.14)
[Click here for the Press Statement](#)
- **Web Notice:** Five (5) new Name/Address change announcement have been posted. (05.08.14)
[Click here to read.](#)
- **Web Notice:** One (1) new Name/Address change announcement has been posted. (05.07.14)
[Click here to read.](#)
- **Web Notice:** One (1) new Name/Address change announcement has been posted. (05.02.14)
[Click here to read.](#)

[Back to Top](#)

April

- **DTAG:** Minutes and presentations from the January 16, 2014 Plenary have been posted (04.29.14)
[Click here to read.](#)
- **Federal Register Notice:** Amendment to the International Traffic in Arms Regulations: Changes to Authorized Officials and the UK Defense Trade Treaty Exemption; Correction of Errors in Lebanon Policy and Violations; and Adoption of Recent Amendments as Final; Correction has been posted. (04.23.14)
[Click here to read.](#)
- **Federal Register Notice:** Amendment to the International Traffic in Arms Regulations: Central African Republic has been posted. (04.23.14)
[Click here to read.](#)
- **Frequently Asked Questions:** Various FAQs have been updated. (04.23.14)
[Click here to read.](#)
- **Web Notice:** Two (2) new Name/Address change announcement have been posted. (04.22.14)
[Click here to read.](#)
- **Industry Notice:** *Realignment of USML Category VII - Ground Vehicles*
Effective on Apr 21, 2014, the Office of Defense Trade Controls Licensing will temporarily realign responsibility for the review and adjudication of export license applications and other written requests related to U.S. Munitions List (USML) Category VII - Ground Vehicles to the Aircraft Division. Any cases under review at the effective date will continue to be reviewed by the assigned Licensing Officer. Industry action is not required in response to this change as the realignment will be handled automatically when cases are submitted. (04.21.14)
- **Web Notice:** Two (2) new Name/Address change announcement have been posted. (04.18.14)
[Click here to read.](#)
- **Web Notice:** Two (2) new Name/Address change announcement have been posted. (04.14.14)
[Click here to read.](#)
- **Web Notice:** One (1) new Name/Address change announcement has been posted. (04.07.14)
[Click here to read.](#)
- **Web Notice:** Two (2) new Name/Address change announcement have been posted. (04.02.14)
[Click here to read.](#)
- **DTrade:** The IBM Forms Viewer used to view, complete, and sign DTrade forms has been updated to version 8.0.1.1. DTrade users must **uninstall** the existing version (v8.0.1) before installing the new version. (04.02.14)
[Click here to download the new viewer](#) once the previous version has been uninstalled.
- **Web Notice:** Two (2) new Name/Address change announcement have been posted. (04.01.14)
[Click here to read.](#)

[Back to Top](#)

March

- **Web Notice:** One (1) new Name/Address change announcement has been posted. (03.31.14)
[Click here to read.](#)
- **Industry Notice:** The Department of State has placed a hold on the issuance of licenses that would authorize the export of defense articles and defense services to Russia. State will continue this practice until further notice. (03.27.14)
- **Web Notice:** One (1) new Name/Address change announcement has been posted. (03.28.14)
[Click here to read.](#)
- **Industry Notice:** DS2032 Registration Submitters: Due to a recent glitch with registration submissions, the Directorate of Defense Trade Controls (DDTC) requests that any DS2032 registration submitted between 3:50 pm on June 25, 2014 and 9:30 am on June 26, 2014 (i.e., transaction receipts ending in 860 through 893) be resubmitted via the Electronic Forms Submission page (<https://dtas-online.pmdtcc.state.gov/>). Be advised that no breach of information occurred and the anomaly has been corrected. We regret any inconvenience this may have caused.(03.27.14)
- **Export Control Reform BIS Seminars:** The Bureau of Industry and Security will conduct a series of briefings to help companies understand how to comply with the different regulatory requirements in the Export Administration Regulations (EAR). The next programs will be conducted in Los Angeles, CA on April 15, 2014, and in Seattle, WA on April 17, 2014. For additional details regarding the upcoming seminars, [click here](#). (03.27.14)
- **Web Notice:** Two (2) new Name/Address change announcement have been posted. (03.27.14)
[Click here to read.](#)
- **Web Notice:** One (1) new Name/Address change announcement has been posted. (03.20.14)
[Click here to read.](#)
- **Licensing:** The Approved Foreign Persons and Approved Space Programs for COMSAT Exports to U.S. Allies (22 CFR §123.27) have been updated. (03.20.14)
[Click here for more information.](#)
- **Web Notice:** One (1) new Name/Address change announcement has been posted. (03.19.14)
[Click here to read.](#)
- **Web Notice:** Two (2) new Name/Address change announcement have been posted. (03.11.14)
[Click here to read.](#)
- **Web Notice:** One (1) new Name/Address change announcement has been posted. (03.07.14)
[Click here to read.](#)
- **Compliance:** Esterline Technologies Corporation consent agreement has been posted. (03.06.14)
[Click here to read.](#)
- **Web Notice:** One (1) new Name/Address change announcement has been posted. (03.06.14)
[Click here to read.](#)

[Back to Top](#)

February

- **Web Notice:** One (1) new Name/Address change announcement has been posted. (02.28.14)
[Click here to read.](#)
- **Treaties:** Australia - United States Defence Trade Cooperation Treaty, Government of Australia End-Use List has been updated. (02.26.14)
[Click here to read.](#)
- **Web Notice:** One (1) new Name/Address change announcement has been posted. (02.18.14)
[Click here to read.](#)
- **DTAG:** Notice of Membership. The U.S. Department of State's Bureau of Political-Military Affairs is accepting membership applications for the 2014 ♦ 2016 DTAG. The Bureau of Political-Military Affairs is interested in applications from subject matter experts from the United States defense industry, relevant trade and labor associations, academic, and foundation personnel. (02.12.14)
[Click here to read.](#)
- **Federal Register Notice:** Amendment to the International Traffic in Arms Regulations: Changes to Authorized Officials and the UK Defense Trade Treaty Exemption; Correction of Errors in Lebanon Policy and Violations; and Adoption of Recent Amendments as Final has been posted. (02.11.14)
[Click here to read.](#)

- **Web Notice:** Three (3) new Name/Address change announcement have been posted. (02.03.14)
[Click here to read.](#)

[Back to Top](#)

January

- **Web Notice:** Three (3) new Name/Address change announcement have been posted. (01.29.14)
[Click here to read.](#)
- **Web Notice:** Two (2) new Name/Address change announcement have been posted. (01.24.14)
[Click here to read.](#)
- **Web Notice:** One (1) new Name/Address change announcement has been posted. (01.14.14)
[Click here to read.](#)
- **Export Control Reform:** The Export Control Reform (ECR) FAQs have been updated. (01.14.14)
[Click here to read.](#)
- **Web Notice:** One (1) new Name/Address change announcement has been posted. (01.09.14)
[Click here to read.](#)
- **Web Notice:** One (1) new Name/Address change announcement has been posted. (01.07.14)
[Click here to read.](#)
- **Treaties:** HMG Projects List for U.S.-UK Defence Trade Cooperation Treaty has been updated. (01.07.14)
[Click here to read.](#)
- **Export Control Reform:** Major Export Control Reform regulation takes effect today, January 6, 2014. The rule, [78 FR 40922](#), Public Notice 8370, amends USML Categories VI, VII, XIII, XX, adds new definitions and makes other changes to the ITAR. (01.06.14)
- **Industry Notice:** In support of Federal Register Notice 78 FR 40922, all DTrade DSP forms, DS2032, and the Common Schema have been upgraded to accommodate the additions and revisions to USML Categories VI, VII, XIII, and XX. Beginning January 6, 2014, DTrade users must use version 8.1 for the DSP-5, 6, 61, 62, and 74 and version 8.2 for the DSP-73 to submit license applications and amendment forms; registrants must use version 4.1 to submit the DS2032; and the Common Schema has been updated to version 7.1, earlier versions of these forms and schema will automatically be rejected by the system.
If you have any questions related to this announcement, please contact the DDTC Help Desk at 202-663-2838 or DTradeHelpDesk@state.gov. (01.03.14)
- **Federal Register Notice:** Amendment to the International Traffic in Arms Regulations: Third Rule Implementing Export Control Reform has been posted. (01.02.14)
[Click here to read.](#)
- **Federal Register Notice:** Amendment to the International Traffic in Arms Regulations: Continued Implementation of Export Control Reform; Correction has been posted. (01.02.14)
[Click here to read.](#)

[Back to Top](#)

EXHIBIT 6

268

AM. AND ATTORNEY GENERAL
CRIMINAL JUSTICE DIVISION

Department of Justice
Washington, D.C. 20530

11-18-78
11-18-78

MEMORANDUM TO DR. FRANK PRESS
Science Advisor to the President

Re: Constitutionality Under the First Amendment
of ITAR Restrictions on Public Cryptography

The purpose of this memorandum is to discuss the constitutionality under the First Amendment of restrictions imposed by the International Traffic in Arms Regulation (ITAR), 22 C.F.R. § 121 et seq. (1977), the regulation implementing § 38 of the Arms Export Control Act, 22 U.S.C.A. § 2778 (1977), on dissemination of cryptographic information developed independent of government supervision or support by scientists and mathematicians in the private sector.^{1/} Our discussion is confined to the applicability of the regulation to the speech elements of public cryptography, and does not address the validity of the general regulatory controls over exports of arms and related items. We have undertaken our review of the First Amendment issues raised by the ITAR as an outgrowth of our role in implementing Presidential Directive NSC-24.^{2/}

^{1/} The cryptographic research and development of scientists and mathematicians in the private sector is known as "public cryptography." As you know, the serious concern expressed by the academic community over government controls of public cryptography, see, e.g., 197 Science 1345 (Sept. 30, 1977), led the Senate Select Committee on Intelligence to conduct a recently concluded study of certain aspects of the field.

^{2/} Our research into the First Amendment issues raised by government regulation of public cryptography led tangentially into broader issues of governmental control over dissemination of technical data. Those questions are numerous, complex, and deserving of extensive study, but are beyond the scope of this memorandum.

participation in briefings and symposia) and disclosed to foreign nationals in the United States (including plant visits and participation in briefings and symposia).

Thus ITAR requires licensing of any communication of cryptographic information,^{4/} whether developed by the government or by private researchers, which reaches a foreign national.^{5/}

The standards governing license denial are set out in § 123.05. The Department of State may deny, revoke, suspend or amend a license:

whenever the Department deems such action to be advisable in furtherance of (1) world peace; (2) the security of the United States; (3) the foreign policy of the United States; or (4) whenever the Department has reason to believe that section 414 of the Mutual Security Act of 1954, as amended, or any regulation contained in this subchapter shall have been violated.

Upon any adverse decision, the applicant may present additional information and obtain a review of the case by the

^{4/} The ITAR does exempt from the licensing requirement unclassified technical data available in published form. 22 C.F.R. § 125.11(a). The scope of that exemption is somewhat unclear, although it does appear that the burden of ascertaining the ITAR status of possibly exempt information is on the individual seeking publication. See 22 C.F.R. § 125 n.3. In order to claim the exemption, an "exporter" must comply with certain certification procedures. 22 C.F.R. § 125.22.

^{5/} For example, in one instance the Office of Munitions Control, the office in the State Department which administers the ITAR, refused to issue licenses to a group of scientists preparing to address a conference on space technology in Madrid. The scientists, who had already arrived in Spain, were refused permission to deliver papers at the symposium on the subject of rocket propulsion and re-entry problems of space vehicles. Note, Arms Control-State Department Regulation of Exports of Technical Data Relating to Munitions Held to Encompass General Knowledge and Experience, 9 N.Y.U. Int'l Law J. 91, 101 (1976).

ITAR Provisions and Statutory Authority

Under the ITAR, exports of articles designated on the United States Munitions List as "arms, ammunition, and implements of war" must be licensed by the Department of State. 22 C.F.R. §§ 123, 125. Cryptographic devices are included on the list, 22 C.F.R. § 121.01, Category XIII, as are related classified and unclassified technical data, Category XVII, Category XVIII. It is this control over the export of unclassified technical data which raises the principal constitutional questions under the ITAR.^{3/}

The broad definition of the term technical data in the ITAR includes:

Any unclassified information that can be used, or be adapted for use, in the design, production, manufacture, repair, overhaul, processing, engineering, development, operation, maintenance, or reconstruction of arms, ammunition and implements of war on the U.S. Munitions List.

22 C.F.R. § 125.01. The definition of the term "export" is equally broad. Under § 125.03 of the ITAR an export of technical data takes place:

Whenever technical data is inter alia, mailed or shipped outside the United States, carried by hand outside the United States, disclosed through visits abroad by American citizens (including

^{3/} Unclassified technical data would generally encompass only privately developed, nongovernmental cryptographic research. It is our understanding that government-sponsored cryptographic research traditionally has been classified. The only unclassified government cryptographic information of which we are aware is the Data Encryption Standard (DES) algorithm. The DES was developed for public use by IBM with National Security Agency assistance and published in the Federal Register by the National Bureau of Standards.

Department. § 123.05(c). No further review is provided.

Nearly all of the present provisions of the ITAR were originally promulgated under § 414 of the Mutual Security Act of 1954 (former 22 U.S.C. § 1934). That statute gave the President broad authority to identify and control the export of arms, ammunition, and implements of war, including related technical data, in the interest of the security and foreign policy of the United States. Congress recently substituted for that statute a new § 38 of the Arms Export Control Act, 22 U.S.C.A. § 2778 (1977), as amended, 22 U.S.C.A. § 2778 (Supp. 3 1977). This statute substitutes the term "defense articles and defense services" for the term "arms, ammunition, and implements of war."^{6/} The President delegated his authority under both statutes to the Secretary of State and Secretary of Defense. Exec. Order No. 11,958, 42 Fed. Reg. 4311 (1977), reprinted in 22 U.S.C.A. § 2778 (Supp. 1 1977); Exec. Order No. 10,973, 3 C.F.R. 493 (Supp. 1964). A willful violation of § 38 of the Arms Export Control Act or any regulation thereunder is punishable by a fine up to \$100,000, imprisonment up to two years, or both. 22 U.S.C.A. § 2778(c).^{7/}

^{6/} The ITAR has not yet been amended to reflect the statutory change. We understand, however, that the Department of State has nearly completed a draft revision of the ITAR. It is our understanding that the revision is not intended to make any major substantive changes in the ITAR, but rather to update and clarify the regulatory language.

^{7/} Although the focus of this memorandum is on the First Amendment issues raised by the ITAR, we feel that one comment about the breadth of the two statutes is in order. It is by no means clear from the language or legislative history of either statute that Congress intended that the President regulate noncommercial dissemination of information, or considered the problems such regulation would engender. We therefore have some doubt whether § 38 of the Arms Export Control Act provides adequate authorization for the broad controls over public cryptography which the ITAR imposes.

The First Amendment Issues

The ITAR requirement of a license as a prerequisite to "exports" of cryptographic information clearly raises First Amendment questions of prior restraint.^{8/} As far as we have been able to determine, the First Amendment implications of the ITAR have received scant judicial attention.

The Ninth Circuit presently has a case under consideration which squarely presents a First Amendment challenge to the ITAR and could serve as a vehicle for the first comprehensive judicial analysis of its constitutionality. In that case, United States v. Edler, No. 76-3370, the defendants, Edler Industries, Inc. and Vernon Edler its president, were charged with exporting without a license technical data and assistance relating to the fabrication of missile components. Although the State Department had denied defendants an export license to provide technical data and assistance to a French aerospace firm, the government alleged that defendants nonetheless delivered data and information to the French during meetings in both France and the United States. Defendants were tried before a jury and found guilty. The trial court, the United States District Court for the Central District of California, did not issue an opinion in the case. On appeal, the defendants contend that the ITAR is both overbroad and establishes an unconstitutional prior restraint. The government's rejoinder to those claims is that the ITAR licensing provisions involve conduct not speech and that any effect upon First Amendment freedoms is merely incidental

^{8/} In addition, the regulatory provisions present questions of overbreadth and vagueness. "Overbreadth" is a First Amendment doctrine invalidating statutes which encompass, in a substantial number of their applications, both protected and unprotected activity. The "vagueness" concept, on the other hand, originally derives from the due process guarantee, and applies where language of a statute is insufficiently clear to provide notice of the activity prohibited. The same statute or regulation may raise overlapping questions under both doctrines.

and therefore valid. We anticipate that the resolution of these issues by the Ninth Circuit may provide substantial guidance as to the First Amendment implications of the ITAR.^{9/}

The only published decision addressing a First Amendment challenge to the ITAR of which we are aware is United States v. Donas-Botto, 363 F.Supp. 191 (E.D. Mich. 1973), aff'd sub nom. United States v. Van Hee, 531 F.2d 352 (6th Cir. 1976). The defendants in that case were charged with conspiracy to export technical data concerning a Munitions List item without first obtaining an export license or written State Department approval. The exports by the defendants both of blueprints and of their technical knowledge concerning an armored amphibious vehicle were alleged to be in violation of § 414 of the Mutual Security Act and the ITAR. In a motion to dismiss the indictments, defendants contended that inclusion of technical knowledge within the statute violated the First Amendment. The trial court disposed of that contention summarily, stating:

[W]hen matters of foreign policy are involved the government has the constitutional authority to prohibit individuals from divulging "technical data" related to implements of war to foreign governments.

363 F. Supp. at 194. The Sixth Circuit upheld the conviction of one of the defendants without reaching any First Amendment questions since none was presented on appeal.^{10/}

The First Amendment analysis of the ITAR in the case thus is limited to a paragraph in the district court's opinion. In reaching the conclusion that the prosecutions did not violate the First Amendment, that court relied upon two Espionage Act decisions, Corin v. United States, 312 U.S.

^{9/} We understand that the case was argued this past March.

^{10/} The court did agree with the trial judge that the ample scope of the term "technical data" in the ITAR encompassed unwritten technical knowledge. 531 F.2d at 537.

19 (1941), and United States v. Rosenberg, 195 F.2d 583 (2d Cir.), cert. denied, 344 U.S. 838 (1952). While those cases establish that the First Amendment does not bar prosecutions for disclosing national defense information to a foreign country, they by no means resolve the prior restraint question.^{11/}

A decision in a somewhat analogous area, the use of secrecy agreements by government agencies as a means of protecting against the unauthorized disclosure of information by present or former employees, while not directly applicable to the First Amendment questions we confront under the ITAR, is helpful for its discussion of government's power to control the dissemination of government information. That case, United States v. Marchetti, 466 F.2d 1309 (4th Cir.), cert. denied, 409 U.S. 1063 (1972), after remand, Alfred A. Knopf, Inc. v. Colby, 509 F.2d 1362 (4th Cir.), cert. denied, 421 U.S. 992 (1975), involved an action for an injunction brought by the United States to prevent a former CIA agent from publishing certain information he had obtained as a result of his CIA employment. The court held that the particular secrecy agreement was valid and enforceable in spite of Marchetti's First Amendment objections, but observed that:

The First Amendment limits the extent to which the United States, contractually or otherwise, may impose secrecy agreements upon its employees and enforce them with a system of prior censorship. It precludes such restraints with respect to information which is unclassified or officially disclosed.

Id. at 1313. The general principle we derive from the case is that a prior restraint on disclosure of information generated by or obtained from the government is justifiable under the First Amendment only to the extent that the information is properly classified or classifiable.

^{11/} It is not clear from reading the district court's opinion on what First Amendment ground or grounds the defendants based their unsuccessful motion to dismiss.

Our research into areas in which the government has restricted disclosure of nongovernmental information provided little additional guidance. Perhaps the closest analogy to controls over public cryptography are the controls over atomic energy research.^{12/} Under the Atomic Energy Act of 1954, 42 U.S.C. § 2011 et seq. (1970), all atomic energy information, whether developed by the government or by private researchers, is automatically classified at its creation and subjected to strict nondisclosure controls.^{13/} Although neither the Atomic Energy Act nor its accompanying regulations establish formal procedures for prior review of proposed atomic energy publications, the Atomic Energy Commission (whose functions are now divided

^{12/} Atomic energy research is similar in a number of ways to cryptographic research. Development in both fields has been dominated by government. The results of government created or sponsored research in both fields have been automatically classified because of the imminent danger to national security flowing from disclosure. Yet meaningful research in the fields may be done without access to government information. The results of both atomic energy and cryptographic research have significant nongovernmental uses in addition to military use. The principal difference between the fields is that many atomic energy researchers must depend upon the government to obtain the radioactive source materials necessary in their research. Cryptographers, however, need only obtain access to an adequate computer.

^{13/} See Green, Information Control and Atomic Power Development, 21 Law and Contemporary Problems 91 (1956); Newman, Control of Information Related to Atomic Energy, 56 Yale L.J. 769 (1947). The Atomic Energy Act uses the term "Restricted Data" to describe information which the government believes requires protection in the interest of national security. "Restricted data" is defined in 42 U.S.C. § 2014(4). The information control provisions of the Act are set out at 42 U.S.C. §§ 2161-2164.

between the Nuclear Regulatory Commission and the Department of Energy) has been empowered to maintain control over publications through threat of injunction or of heavy criminal penalties, two potent enforcement tools provided under the Act. 42 U.S.C. §§ 2271-2277, 2280. It does not seem, however, that the broad information controls of the Atomic Energy Act have ever been challenged on First Amendment grounds. Our search for judicial decisions in other areas in which the government has imposed controls over the flow of privately generated information was equally unavailing.^{14/}

In assessing the constitutionality of the ITAR restrictions on the speech elements of public cryptography we therefore have turned to Supreme Court decisions enunciating general First Amendment principles. It is well established that prior restraints on publication are permissible only in extremely narrow circumstances and that the burden on the government of sustaining any such restraint is a heavy one. See, e.g., Nebraska Press Association v. Stuart, 427 U.S. 539 (1976); New York Times Co. v. United States, 403 U.S. 713 (1971); Organization for a Better Austin v. Keefe, 402 U.S. 415 (1971); Carroll v. Princess Anne, 393 U.S. 175 (1968); Near v. Minnesota, 283 U.S. 697 (1931). Even in those limited circumstances in which prior restraints have been deemed constitutionally permissible, they have been circumscribed by specific, narrowly drawn standards for deciding whether to prohibit disclosure and by substantial procedural protections. Erznoznik v. City of Jacksonville, 422 U.S. 205 (1975); Blount v. Rizzi, 400 U.S. 410 (1971); Freedman v. Maryland, 380 U.S. 51 (1965); Niemotko v. Maryland,

^{14/} For example, it does not appear that the broad controls over exports of technical data and related information under the Export Administration Act of 1969, 50 U.S.C. App. § 2401 et seq. (1970), and accompanying regulations have been judicially tested on First Amendment grounds. Nor have the provisions of the patent laws restricting patentability of inventions affecting national security, 35 U.S.C. § 181 et seq. (1970), nor governmental restrictions on communications with Rhodesia, 22 U.S.C. § 287c (1970); Exec. Order No. 11,322

340 U.S. 268 (1951); Kunz v. New York, 340 U.S. 290 (1951); Hague v. C.I.O., 307 U.S. 496 (1939).^{15/}

Even if it is assumed that the government's interest in regulating the flow of cryptographic information is sufficient to justify some form of prior review process, the existing ITAR provisions we think fall short of satisfying the strictures necessary to survive close scrutiny under the First Amendment. There are at least two fundamental flaws in the regulation as it is now drawn: first, the standards governing the issuance or denial of licenses are not sufficiently precise to guard against arbitrary and inconsistent administrative action; second, there is no mechanism established to provide prompt judicial review of State Department decisions barring disclosure. See, e.g., Blount v. Rizzi, supra; Freedman v. Maryland, supra; Hague v. C.I.O., supra. The cases make clear that before any restraint upon protected expression may become final it must be subjected to prompt judicial review in a proceeding in which the government will bear the burden of justifying its decisions. The burden of bringing a judicial proceeding cannot be imposed upon those desiring export licenses in these circumstances. The ITAR as presently written fails to contemplate this requirement.^{16/}

^{15/} In Freedman, 380 U.S. at 58-59, the Court summarized the procedural protections necessary to sustain a scheme of prior review:

1. A valid final restraint may be imposed only upon a judicial determination;
2. The administrator of a licensing scheme must act within a specified brief period of time;
3. The administrator must be required either to issue a license or go to court to seek a restraint;
4. Any restraint imposed in advance of a final judicial determination on the merits must be limited to preservation of the status quo for the shortest period compatible with sound judicial resolution;
5. The licensing scheme must assure a prompt final judicial decision reviewing any interim and possibly erroneous denial of a license.

^{16/} The government's argument to the Ninth Circuit in Edler, that the impact of the ITAR upon protected communications is merely incidental, and that the ITAR should be viewed as

(Cont. on p. 11)

For these reasons it is our conclusion that the present ITAR licensing scheme does not meet constitutional standards. There remains the more difficult question whether a licensing scheme covering either exports of or even purely domestic publications of cryptographic information might be devised consistent with the First Amendment. Recent Supreme Court decisions certainly suggest that the showing necessary to sustain a prior restraint on protected expression is an onerous one. The Court held in the Pentagon Papers case that the government's allegations of grave danger to the national security provided an insufficient foundation for enjoining disclosure by the Washington Post and the New York Times of classified documents concerning United States activities in Vietnam. New York Times Co. v. United States, supra.^{16/} The Court also invalidated prior restraints when justified by such strong interests as the right to fair trial, Nebraska Press Ass'n, supra, and the right of a homeowner to privacy, Organization for a Better Austin v. Keefe, supra. Such decisions raise a question whether a

16/ (Cont.)

a regulation of conduct not speech, deserves note. According to that argument, the less rigorous constitutional standard of United States v. O'Brien, 391 U.S. 367 (1968), would govern the validity of the ITAR. Although that may be true with respect to certain portions of the ITAR, even a cursory reading of the technical data provisions reveals that those portions of the ITAR are directed at communication. A more stringent constitutional analysis than the O'Brien test is therefore mandated.

17/ The Pentagon Papers case produced a total of ten opinions from the Court, a per curiam and nine separate opinions. All but Justices Black and Douglas appeared willing to accept prior restraints on the basis of danger to the national security in some circumstances. There was, however, no agreement among the Justices on the appropriate standard. Justice Brennan stated his view that a prior restraint on publication was justified only upon:

"proof that publication must inevitably, directly, and immediately cause the occurrence of an event kindred to imperiling the safety of a transport already at sea. . . ."

(Cont. on p. 12)

generalized claim of threat to national security from publication of cryptographic information would constitute an adequate basis for establishing a prior restraint. Nonetheless, it is important to keep in mind that the Court has consistently rejected the proposition that prior restraints can never be employed. See, e.g., Nebraska Press Ass'n, *supra* at 570. For example, at least where properly classified government information is involved, a prior review requirement may be permissible. United States v. Marchetti, *supra*.

In evaluating the conflicting First Amendment and national security interests presented by prior restraints on public cryptography, we have focused on the basic values which the First Amendment guarantees. At the core of the First Amendment is the right of individuals freely to express political opinions and beliefs and to criticize the operations of government. See, e.g., Landmark Communications v. Virginia, 46 U.S.L.W. 4389, 4392 (May 1, 1978); Buckley v. Valeo, 424 U.S. 1, 14 (1976); Mills v. Alabama, 384 U.S. 214, 218 (1966). Adoption of the Amendment reflected a "profound national commitment to the principle that debate on public issues should be uninhibited, robust, and wide-open," New York Times v. Sullivan, 376 U.S. 254, 270 (1964), and was intended in part to prevent use of seditious libel laws to stifle discussion of information embarrassing to the government. New York Times Co. v. United States, *supra* at 724 (concurring opinion of Mr. Justice Douglas).

Prior restraints pose special and very serious threats to open discussion of questions of public interest. "If it can be said that a threat of criminal or civil sanctions after publication 'chills' speech, prior restraint 'freezes' it at least for the time." Nebraska Press Ass'n, *supra* at 559.

17/ (Cont.)

403 U.S. at 726-27. Justice Stewart, with whom Justice White concurred, suggested that a prior restraint would be permissible only if disclosure would "surely result in direct, immediate and irreparable damage to our Nation or its people." *Id.* at 730. Several other Justices declined, given the facts and procedural posture of the case, to formulate a standard.

Since views on governmental operations or decisions often must be aired promptly to have any real effect, even a temporary delay in communication may have the effect of severely diluting "uninhibited, robust, and wide-open" debate. And protection of any governmental interest may usually be accomplished by less restrictive means. One avenue generally available to the government, and cited by Supreme Court as the most appropriate antedote, is to counter public disclosures or criticisms with publication of its own views. See, e.g., Whitney v. California, 274 U.S. 357, 375 (1927) (concurring opinion of Mr. Justice Brandeis).

The effect of a prior restraint on cryptographic information, however, differs significantly from classic restraints on political speech. Cryptography is a highly specialized field with an audience limited to a fairly select group of scientists and mathematicians. The concepts and techniques which public cryptographers seek to express in connection with their research would not appear to have the same topical content as ideas about political, economic or social issues. A temporary delay in communicating the results of or ideas about cryptographic research therefore would probably not deprive the subsequent publication of its full impact.

Cryptographic information is, moreover, a category of matter "which is both vital and vulnerable to an almost unique degree."^{18/} Once cryptographic information is disclosed, the damage to the government's interest in protecting

^{18/} New York Times Co. v. United States, 403 U.S. 713, 736 n. 7 quoting H.R. Rep. No. 1895, 81st Cong., 2d Sess., 1 (1950). That report pertains to the bill which became 18 U.S.C. § 798, the criminal statute prohibiting disclosure of information concerning the cryptographic systems and communications intelligence activities of the United States. Section 798 does not reach disclosure of information published by public cryptographers, as its coverage is restricted to classified information. Classified information by definition is information in which the government has some proprietary interest. See § 1(b) of the May 3, 1978 draft of the Executive Order on national security proposed to replace Executive Order 11,652; cf. 22 C.F.R. § 125.02.

national security is done and may not be cured. Publication of cryptographic information thus may present the rare situation in which "more speech" is not an alternative remedy to silence.^{19/} See Whitney v. California, supra at 376 (concurring opinion of Mr. Justice Brandeis).

Given the highly specialized nature of cryptographic information and its potential for seriously and irremediably impairing the national security, it is our opinion that a licensing scheme requiring prepublication submission of cryptographic information might overcome the strong constitutional presumption against prior restraints. Any such scheme must, as we have said, provide clear, narrowly defined standards and procedural safeguards to prevent abuse.

While a detailed discussion of the specific provisions and procedures of a valid scheme of prior review of cryptographic information or of its practical and political feasibility is beyond the scope of this memorandum, some

^{19/} In stressing the differences between cryptographic information and other forms of expression we do not mean to imply that the protections of the First Amendment are not applicable to cryptographic information or that they are confined to the exposition of ideas. See Winters v. New York, 333 U.S. 507, 510 (1948). We recognize that the scope of the amendment is broad. It encompasses, for example, purely commercial speech, Virginia State Board of Pharmacy v. Virginia Citizens Consumer Council, Inc. 425 U.S. 748 (1976), and communicative conduct, Cohen v. California 403 U.S. 15 (1971). We believe, however, that the extent of First Amendment protection may vary depending upon the nature of communication at issue. It is established in the area of commercial speech that greater governmental regulation may be tolerated due to the special attributes of that form of speech. Virginia State Board of Pharmacy v. Virginia Citizens Consumer Council, supra at 770-71 and n.24. Speech in the labor context also presents special First Amendment considerations. See, e.g., N.L.R.B. v. Gissel Packing Co., 395 U.S. 575 (1969). And obscene communications have received specialized treatment from the courts. See, e.g., Roth v. United States, 354 U.S. 476 (1957).

general observations are in order. First, we wish to emphasize our doubts that the executive branch may validly provide for licensing or prior review of exports of cryptographic information without more explicit Congressional authorization. The scope of the existing delegation of authority from Congress to the President, as we note above, is somewhat unclear. Before imposing a prior restraint on exports of public cryptographic information, we believe that a more clear cut indication of Congressional judgment concerning the need for such a measure is in order. See United States v. Robel, 389 U.S. 248, 269 (1967) (concurring opinion of Mr. Justice Brennan); cf. Yakus v. United States, 321 U.S. 414 (1944). Some of S. 11
Vol. 7.

Second, further Congressional authorization would obviously be necessary in order to extend governmental controls to domestic as well as foreign disclosures of public cryptographic information. Such an extension might well be necessary to protect valuable cryptographic information effectively. Indeed, limiting controls to exports while permitting unregulated domestic publication of cryptographic research would appear to undermine substantially the government's position that disclosure of cryptographic information presents a serious and irremediable threat to national security.^{20/}

^{20/} A question which would arise from complete governmental control over cryptographic information is whether the government would be required under the Fifth Amendment to pay just compensation for the ideas it had effectively "condemned." For example, the patent and invention provisions of the Atomic Energy Act require the government to pay for patents which it revokes or declares to be affected with the public interest. 42 U.S.C. §§ 2181-2190. A cryptographic algorithm, however, would not appear to be a patentable process. See Gottschalk v. Benson, 409 U.S. 63 (1972). And it is unresolved whether copyright protection is available for computer software. See Nimmer on Copyright, § 13.1 (Supp. 1976). We are therefore uncertain as to the status of cryptographic ideas under the Fifth Amendment.

Third, no final restraint on disclosure may be imposed without a judicial determination. We recognize that a requirement of judicial review presents substantial problems. The proof necessary in order to demonstrate to a judge that highly technical cryptographic information must be withheld from publication because of the overriding danger to national security might be burdensome and might itself endanger the secrecy of that information. It is our opinion, however, that any system which failed to impose the burden on government of seeking judicial review would not be constitutional.^{21/} See, e.g., Blount v. Rizzi, *supra*.

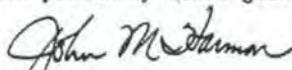
Finally, any scheme for prior review of cryptographic information should define as narrowly and precisely as possible both the class of information which the government must review to identify serious threats to the national security and the class of information which the government must withhold.^{22/} The scheme clearly should exempt from a

^{21/} The threat to national security posed by a judicial review procedure could be reduced substantially by conducting the review in camera. See Alfred A. Knopf, Inc. v. Colby, 509 F.2d 1362 (4th Cir.), *cert. denied*, 421 U.S. 992 (1975); *cf.* 5 U.S.C. 552(a)(4)(B) (Supp. 1975) (in camera review provision of the Freedom of Information Act). The Supreme Court, in any event, has been unimpressed by arguments that disclosure of sensitive national security information to a court raises such serious problems of public dissemination that exemption from constitutional requirements is appropriate. See United States v. U.S. District Court, 407 U.S. 297 (1972).

^{22/} In other words, we assume that the information submitted under the scheme would not be coextensive with the information withheld. We note, however, that the authority of the government to require prepublication submission of information which is neither classified nor classifiable is unsettled. That issue is posed in the suit recently filed by the Department of Justice in the United States District Court for the Eastern District of Virginia against former CIA employee Frank Snepp for breach of his secrecy agreement. United States v. Snepp, Civil Action No. 78-92-A.

submission requirement any information, such as that which is publicly available or which poses no substantial security threat, that the government has no legitimate interest in keeping secret.^{23/} Failure to draft provisions narrowly might well invite overbreadth challenges for inclusion of protected communication. See, e.g., NAACP v. Alabama, 357 U.S. 449 (1958). And a precisely drawn scheme is also necessary to avoid objections of vagueness. See, e.g., Smith v. Goguen, 415 U.S. 566 (1974).^{24/}

In conclusion, it is our view that the existing provisions of the ITAR are unconstitutional insofar as they establish a prior restraint on disclosure of cryptographic ideas and information developed by scientists and mathematicians in the private sector. We believe, however, that a prepublication review requirement for cryptographic information might meet First Amendment standards if it provided necessary procedural safeguards and precisely drawn guidelines.



John M. Harmon
Assistant Attorney General
Office of Legal Counsel

^{23/} As we noted above, at n.4, supra, the present ITAR provisions attempt to exempt publicly available information. But the scope of that exemption and the procedures for invoking it, particularly with respect to oral communications, are somewhat clear.

^{24/} Although we mention questions of overbreadth and vagueness raised by the technical data provisions of the ITAR previously in this memorandum, we have not attempted to identify and analyze particular problems for several reasons. First, our opinion that a prior restraint on public cryptography might survive First Amendment scrutiny is a limited one and does not purport to apply to the many other types of technical data covered by the ITAR. Second, we believe that public cryptography presents special considerations warranting separate treatment from other forms of technical data, and that a precise and narrow regulation or statute limited to cryptography would be more likely to receive considered judicial attention. Finally, we are uncertain whether the present legislative authority for the technical data provisions of the ITAR is adequate.

EXHIBIT 7

Constitutionality of the Proposed Revision of the International Traffic in Arms Regulations

Proposed revision of the "technical data" provision of the International Traffic in Arms Regulations (ITAR) redefines and narrows the class of transactions that are subject to a licensing requirement under the Arms Export Control Act of 1976, in an attempt to avoid imposing a prior restraint on speech protected by the First Amendment; however, even as revised the ITAR can have a number of constitutionally impermissible applications.

The licensing requirement in the ITAR may constitutionally be applied to transactions involving arrangements entered into by exporters to assist foreign enterprises in the acquisition or use of technology; it may also be applied to transactions involving the dissemination of technical data for the purpose of promoting the sale of technical data or items on the Munitions List, since the prior restraint doctrine has only limited applicability to "commercial speech." However, insofar as it could be applied to persons who have no connection with any foreign enterprise, who disseminate technical data in circumstances in which there is no more than a belief or a reasonable basis for believing that the data might be taken abroad by foreign nationals and used there in the manufacture of arms, the licensing requirement is presumptively unconstitutional as a prior restraint on speech protected by the First Amendment.

It is not certain whether a court would find that the revised ITAR are so substantially overbroad as to be void and unenforceable in all their applications, or decide to save the regulations through a narrowing construction. The best legal solution is for the Department of State, not the courts, to narrow the ITAR so as to make it less likely that they will apply to protected speech in constitutionally impermissible circumstances.

July 1, 1981

MEMORANDUM OPINION FOR THE OFFICE OF MUNITIONS CONTROL, DEPARTMENT OF STATE

The views of this Office have been requested concerning the constitutionality of a proposed revision of the "technical data" provisions of the International Traffic in Arms Regulations (ITAR). 45 Fed. Reg. 83,970 (December 19, 1980). On the basis of the analysis set forth below, we conclude that from a constitutional standpoint, the revised ITAR is a significant improvement over the prior version, but that even as revised, it can have a number of unconstitutional applications. We recommend that the proposed revision be modified to minimize or eliminate the number of impermissible applications. Our views are set forth in more detail below.

I. Background

The ITAR are promulgated pursuant to the Arms Export Control Act of 1976 (the Act). 22 U.S.C. § 2778. The Act authorizes the President “to control the import and export of defense articles and defense services and to provide foreign policy guidance to persons of the United States involved in the export and import of such articles and services” and to “designate those items which shall be considered as defense articles and defense services . . . and to promulgate regulations for the import and export of such articles and services.” § 2778(a). Items so designated are placed on the United States Munitions List. Every person engaging in the business of “manufacturing, exporting, or importing” designated defense articles or services must register with the Office of Munitions Control. § 2778(b). No such articles or services may be exported or imported without a license issued in accordance with regulations promulgated under the Act. § 2778(b)(2). Violation of the statute or the regulations promulgated thereunder is a criminal offense. Pursuant to its authority to regulate the export of “defense articles and services,” the Office of Munitions Control has traditionally undertaken to regulate the export of technical *information* relating to the manufacture or use of items on the Munitions List. The “technical data” provisions are the embodiment of that undertaking.

The proposed revision defines technical data to include unclassified information not in the public domain and relating directly to, *inter alia*, the performance of defense services; training in the operation or use of a defense article; and design, production, or manufacture of such an article.¹ In general, the relevant provisions require the issuance of a license for the export of any unclassified technical data. A license is not, however, required for the export of unclassified technical data included within certain specified categories of exemption. Among those categories are exports of data published or generally available to the public,² exports in furtherance of a manufacturing license agreed to by

¹ Under § 121.315, “technical data” means

- (a) Unclassified information not in the public domain relating directly to:
 - (1) The design, production, manufacture, processing, engineering, development, operation, or reconstruction of an article; or
 - (2) Training in the operation, use, overhaul, repair or maintenance of an article; or
 - (3) The performance of a defense service (see § 121.32);
- (b) Classified information relating to defense articles or defense services, and
- (c) Information covered by a patent secrecy order

45 Fed. Reg. 83,976 (1980)

² The ITAR exempts technical data if they “are published or otherwise generally available to the public”.

- (i) Through sales at newsstands and bookstores;
- (n) Through subscription, unrestricted purchase, or without cost;
- (ni) Through second class mailing privileges granted by the U.S. Government; or,
- (iv) Are freely available at public libraries.

45 Fed. Reg. 83,985 (1980)

the State Department, and exports related to firearms not in excess of caliber .50. Most importantly for present purposes, the revised provisions exempt technical data which:

consists of information which is not designed or intended to be used, or which could not reasonably be expected to be used, in direct application in the design, production, manufacture, repair . . . of defense articles (for example, general mathematical, engineering, or statistical information not purporting to have or not reasonably expected to be given direct application to defense articles.) An advisory opinion may be sought in case of doubt as to whether technical data is exempt under this category.

45 Fed. Reg. 83,985 (1980).

With reference to technical data, the proposed revision defines the term "export" to include both the sending, transmitting, or removal of technical data from the United States, and the transfer of such data to a foreign national when the transferor knows or has reason to know that the transferred data will be sent, transmitted, or taken out of the United States. Disclosure to a foreign national of technical data relating to "significant military equipment," whether in the United States or abroad, is also an "export." Finally, the proposed revision expressly provides that an "export" occurs when (1) technical data are disclosed to a foreign national abroad or (2) technical data are disclosed to a foreign national in the United States when the transferor knows or has reason to know that the disclosed technical data will be disclosed outside the United States.

II. Discussion

The constitutionality of the ITAR was considered and questioned in a memorandum prepared by this Office in 1978 at the request of Dr. Frank Press, Science Advisor to the President. *See* Memorandum of May 11, 1978, for Dr. Frank Press, Science Advisor to the President, from John M. Harmon, Assistant Attorney General, Office of Legal Counsel entitled "Constitutionality Under the First Amendment of ITAR Restrictions on Public Cryptography." On their face, the previous regulations appeared to establish a general administrative rule that required persons subject to United States jurisdiction to apply to the Department of State for a license before communicating technical data to foreign nationals. The regulations were drafted in such a way that this rule could have been applied not only to persons who undertook to transmit technical data during the sale of arms or technical services abroad, but also to virtually any person involved in a presentation or discussion, here or abroad, in which technical data could reach a foreign national. In all such circumstances, anyone who proposed to

discuss or transmit technical data was, under the ITAR, an “exporter”; and he was therefore required by the ITAR to apply in advance for an administrative license, unless the technical data in question fell within the limited exemptions from regulation.

In the memorandum to Dr. Press, this Office concluded that the ITAR cast such a broad regulatory net that it subjected a substantial range of constitutionally protected speech to the control of the Department of State. Because this control was exercised through a system of administrative licensing—a system of “prior restraint”—we concluded that the relevant regulations were presumptively unconstitutional. We also concluded, however, with particular reference to cryptographic information, that the constitutional difficulties presented by this system of prior restraint might be overcome without limiting the range of transactions to which the ITR purported to apply. The difficulties might be overcome if: (1) the standards governing the issuance or denial of an administrative license were defined more precisely to guard against arbitrary and inconsistent administrative action; and (2) a procedural mechanism was established to impose on the government the burden of obtaining prompt judicial review of any State Department decision barring the communication of cryptographic information.

The present proposal for revision of the ITAR does not attempt to satisfy the second condition described in the previous memorandum. It does, however, redefine the class of transactions that are subject to the licensing requirement. It is therefore necessary to determine whether the redefinition of coverage is sufficiently responsive to the constitutional objections raised by our previous opinion concerning the issue of prior restraint to require a different conclusion. If the redefinition of coverage ensures that the licensing requirement can no longer apply to speech that is constitutionally protected against prior restraint, the concerns expressed in our previous opinion will no longer be relevant to the constitutional analysis. On the other hand, if the redefinition does not significantly contract the coverage, the prior restraint doctrine must be taken into account. We adhere to the positions regarding constitutional limits in this area articulated in the memorandum to Dr. Press. If the revised technical data provisions are drafted so broadly that they impinge on speech that is protected against prior restraint, they are presumptively unconstitutional in their application to the speech. Moreover, if their overbreadth is substantial, they may be void and unenforceable in all their applications, although we cannot fully assess that possibility without examining the constitutional status of the entire range of transactions to which they may apply.

The revised technical data provisions may apply to three general categories of transactions: (1) transactions involving the direct transmission of technical data by an exporter to a foreign enterprise under a contract or other arrangement entered into by the exporter for the

purpose of assisting the foreign enterprise in the acquisition of use of technology; (2) transactions involving the dissemination of technical data for the purpose of promoting or proposing the sale of technical data of items on the Munitions List; and (3) transactions in which an “exporter” who is not otherwise connected or concerned with any foreign enterprise transmits technical data knowing, or having reason to know, that the data may be taken abroad and used by someone there in the manufacture or use of arms.

We have concluded that the application of the revised technical data provisions to transactions in the first two categories described above will not violate the First Amendment prohibition against prior restraint. However, the application of these provisions to transactions in the third category will raise serious constitutional questions. Our ultimate conclusions about the constitutionality of the technical data provisions are set forth, together with our recommendations for revision, in section III below.

(1) *Transactions involving arrangements entered into by exporters to assist foreign enterprises in the acquisition or use of technology.* At its core, the ITAR is designed to control United States firms and individuals who undertake to assist foreign enterprises in the acquisition and use of arms. The purpose of the technical data provisions is to extend that control to transactions in which assistance takes the form of technical advice. Perhaps the most common example of a transaction of that kind is a straightforward commercial arrangement in which an American firm agrees to provide technical information or advice to a foreign firm engaged in the manufacture of an item or items on the Munitions List.³

The leading case involving the constitutionality of the ITAR arose in precisely that context. See *United States v. Edler Industries, Inc.*, 579 F.2d 516 (9th Cir. 1978). In *Edler*, an American firm specializing in aerospace technology, Edler Industries, agreed to provide a French firm with technical assistance and data relating to a tape wrapping program. The Office of Munitions Control denied Edler’s application for export licenses on the ground that exportation of the information in question would violate United States policy as established by the Act. During the pendency of the license applications, and after the denial, Edler proceeded to perform the contract and transmitted the information to the French firm. Edler was then prosecuted under the Act. Edler defended on the ground, among others, that the transmission of technical information under the contract with the French firm was constitutionally protected “speech” and that the government could not require such “speech” to be licensed in advance. The trial court rejected that contention and Edler was convicted.

³ We can imagine more exotic examples that would proceed upon essentially the same legal footing, e.g., a transaction in which an American agent (an “industrial spy”) transmits sensitive technical information to his foreign principal.

On appeal, the Ninth Circuit upheld Edler's defense in part. The court concluded that the definition of "technical data" then appearing in 22 CFR § 125.01 (1977) should be interpreted narrowly in light of the applicable constitutional limitations, § 1934 of the Act,⁴ and the relevant legislative history. Under the Act, the regulations should be construed to bar "only the exportation of technical data significantly and directly related to specific articles on the Munitions List." *Id.* at 521. Moreover, if the information in question "could have both peaceful and military applications," the regulations should be construed to apply only in cases in which the defendant knew or had reason to know that the information was "intended for the prohibited use." *Id.* That construction was necessary "to avoid serious interference with the interchange of scientific and technological information." *Id.* If the regulations and the statute were construed to apply only in the case of knowledge or reason to know of an intended prohibited use, they would not "interfere with constitutionally protected speech." *Id.* They would merely control "the conduct of assisting foreign enterprises to obtain military equipment and related technical expertise," and for that reason they would not impose an unconstitutional prior restraint on speech. *Id.* Finally, although the district court had correctly rejected certain elements of the defendant's First Amendment defense, it had adopted an impermissibly broad construction of the regulations, and therefore the case was ordered retried in accordance with the narrower construction.

On the facts presented, the essential holding of *Edler*—that the previous ITAR could be applied constitutionally to an exporter who had agreed to assist a foreign firm in the development of a new technology, having reason to know that the foreign firm intended to use the technology to manufacture items on the Munitions List—was consistent with the traditional principles the courts have applied in the interpretation of the First Amendment. Indeed, the novelty of *Edler* lay not in that holding, but in the defendant's claim that the transmission of technical information under the agreement with the French firm was constitutionally protected "speech." The courts have consistently held that whenever speech is an "integral part" of a larger transaction involving conduct that the government is otherwise empowered to prohibit or regulate, the First Amendment does not immunize that speech; nor does it bar prior restraint. *See, e.g., Ohralik v. Ohio State Bar Assn.*, 436 U.S. 447, 456 (1978), and cases cited therein; *Giboney v. Empire Storage & Ice Co.*, 336 U.S. 490 (1949). That principle comes into play in a number of contexts: most importantly, where speech is joined with conduct by an agreement or special relationship between

⁴This provision was repealed in 1976 and replaced by the current provision, 22 U.S.C. § 2778. For purposes of the interpretation adopted by the *Edler* court, however, the changes in § 1934 are not material.

the speaker and the actor. For example, under the law of conspiracy, when one individual enters into an agreement with another to rob a bank or to restrain trade and provides the other with the information which facilitates that action, neither the agreement nor the transmission of the information is constitutionally protected. *See id.*

To be sure, there is a doctrinal difficulty in applying this traditional analysis to international transactions of the kind involved in *Edler*. When the defendant in *Edler* agreed to assist the French firm in the development and use of sensitive technology, it was not undertaking to aid that firm in conduct that was itself illicit or unauthorized as a matter of domestic law. Our nation has a compelling interest in suppressing the development and use of sensitive technologies abroad, but it has no general power to “outlaw” the development of technology by foreign enterprises or to require them to apply here for a license before making or using arms. As a matter of domestic law, the government’s only recourse is to control persons subject to United States jurisdiction who would undertake to aid and abet those foreign endeavors.

We believe that the absence of a direct domestic prohibition against the foreign conduct in question here—the foreign manufacture or use of items on the Munitions List—does not create a constitutional barrier to domestic regulation of persons who combine with foreign enterprises to assist them in the development and use of sensitive technology. Even though such assistance may take the form of technical advice, it is, in the *Edler* context, an integral part of conduct that the government has a compelling interest in suppressing by appropriate means. As the *Edler* court held, such assistance is not constitutionally protected speech; and it is not protected by the constitutional prohibition against prior restraint.

We have one further observation concerning the *Edler* case. *Edler* held that the licensing requirement of the previous ITAR could be enforced where: (1) the foreign recipient of technical data intended to use it in the manufacture or use of items on the Munitions List; and (2) the exporter had “reason to know” of that intention. Given the nature of the transaction that was involved in *Edler*, those requirements imposed what the Ninth Circuit considered to be necessary limitations on the power of the government to license the transmission of sensitive technical information under international contracts and combinations.⁵

⁵There is room to doubt whether the concise and somewhat ambiguous language adopted by the *Edler* court in the statement of the applicable rule, *see* 579 F.2d at 521, completely captures the relevant constitutional standard. The *Edler* rule presupposes that the foreign enterprise intends to use technical data in the manufacture or use of arms, and it suggests that the licensing requirement can be enforced only where the exporter has reason to know of that intention. But a respectable argument can be made that the constitutional power of the government to license persons who combine with foreign enterprises to assist directly in the development of sensitive technology abroad is not limited to cases in which the foreign enterprise has a present intention of using that technology in the manufacture of arms. The present intention of the foreign actor is constitutionally relevant, of course, but the actual source of the danger is the technical capacity that his action creates. That capacity is created on

Continued

They should be read in that context. We believe they cannot be read as implicitly authorizing the imposition of a general licensing requirement in every circumstance in which a speaker may have known or had reason to know that his speech could be used for a dangerous purpose by someone abroad. Beyond the *Edler* context—a context in which “speech” is joined with dangerous conduct by an actual agreement or combination between speaker and actor—constitutional principles far more favorable to the speaker come into play. We will discuss those principles in part (3) below.

(2) *Transactions involving the dissemination of technical data for the purpose of promoting or proposing the sale of technical data or items on the munitions list.* In this section, we consider the dissemination of technical data for the purpose of promoting or proposing the sale of technical data or items on the Munitions List.⁶ The Supreme Court has given special consideration to promotional materials in a series of recent decisions. Under the rubric of “commercial speech,” information that proposes or promotes a commercial transaction has been accorded some constitutional protection. See *Virginia State Bd. of Pharmacy v. Virginia Citizens Consumer Counsel, Inc.*, 425 U.S. 748 (1976); *Friedman v. Rogers*, 440 U.S. 1 (1979); *Central Hudson Gas v. Public Service Comm’n*, 447 U.S. 557 (1980); *Linmark Associates, Inc. v. Willingboro*, 431 U.S. 85 (1977). Commercial speech is protected because it “assists consumers and furthers the societal interest in the fullest possible dissemination of information.” See *Central Hudson Gas*, *supra*, at 561–62. At the same time, it has been suggested by the Court that commercial speech is in some circumstances entitled to a “lower level” of protection than that accorded to other forms of protected speech. The courts have said that a “lower level” of protection is justified because “commercial speakers have extensive knowledge of both the market and their products” and are thus “well situated to evaluate the accuracy of their messages and the lawfulness of the underlying activity,” and because “commercial speech, the offspring of economic self-interest, is a hardy breed of expression that is not ‘particularly susceptible to being crushed by overbroad regulation.’” *Id.* at 564 n.6 (citation omitted). These factors have led the Supreme Court to conclude that the govern-

foreign soil, beyond the legislative jurisdiction of the United States, and our government may have no adequate means of controlling its subsequent use in a way that will protect against a change of circumstance or intention. Accordingly, one could argue that our nation has a substantial interest in suppressing the creation of foreign capacity in the first instance, whatever the present intentions of the foreign enterprise may be; and if a United States technical expert, knowing of the potential danger, combines with the foreign enterprise to create that capacity, that is arguably enough. An analogous principle is operative in the law of espionage. The transmission of sensitive information by a domestic agent to his foreign principal is not constitutionally protected even where the purpose of the transaction is merely to benefit the foreign power, not to injure the United States. As the Supreme Court noted in the leading case, the status of foreign governments may change; no advantage can be given to them without creating a potential for injury to us. See *Gorn v. United States*, 312 U.S. 19, 30 (1941).

⁶ We are advised by the Federal Bureau of Investigation that technical data are sometimes disseminated in international conferences or meetings for the purpose of promoting the sale of sensitive technology.

ment may ban false or misleading commercial speech, see *Friedman v. Rogers, supra*, at 13, 15–16, and, in at least some contexts, commercial speech relating to illegal activity, *Pittsburgh Press Co. v. Pittsburgh Comm’n on Human Relations*, 413 U.S. 376, 388 (1973). Similar considerations have led the Court to suggest in dicta that the ordinary First Amendment prohibitions against overbreadth and prior restraint may not be fully applicable to commercial speech. See *Virginia State Bd. of Pharmacy, supra*, at 772 n.24.

For purposes of the present discussion, we need not determine whether the prior restraint doctrine is inapplicable to all commercial speech in all circumstances. In the present context, we believe that a licensing requirement for promotional speech that contains technical data would probably be held constitutional. There are four reasons for this conclusion. First, the governmental interest in preventing the development of military equipment by foreign countries is a significant one. That interest may justify prior restraint against the promotion of foreign technical sales in the same way that the national interest in truth and fair dealing justifies prior restraint against false and deceptive promotions in the ordinary commercial context. See *Donaldson v. Read Magazine*, 333 U.S. 178, 189–91 (1948); *FTC v. Standard Education Society*, 302 U.S. 112 (1937). Second, a licensing requirement for promotional materials containing technical data will not delay the transmission of information that the public has a strong interest in receiving immediately. In that respect, technical promotions are unlike political speech, for the public will not generally suffer if technical data are suppressed during a licensing period. Compare *New York Times v. United States, supra*. Third, the protection accorded to commercial speech is largely designed to protect the rights of listeners and consumers. See *Virginia State Bd., supra*. Those rights are not directly implicated here. Foreign enterprises engaged in the manufacture or use of arms abroad generally have no right under the Constitution to receive information from persons in this country. Finally, the Court has indicated that deference to the political branches is most appropriate in the area of military affairs. Cf. *Rostker v. Goldberg*, 453 U.S. 57 (1981); *Brown v. Glines*, 444 U.S. 348 (1980).⁷ On the basis of these factors, and the intimation in *Virginia State Bd.* that the strong presumption against prior restraints may not be fully operable in the commercial context, we believe that the courts would, in general, uphold a licensing requirement for promotional speech that contains technical data.

Whether the “commercial speech” doctrine has any other bearing upon the constitutionality of the technical data provisions is not entirely

⁷ Because Congress’ determinations are of special importance here, it would be useful to obtain clear and specific legislative authority for the technical data regulations. In addition, it may be advisable to provide remedies other than criminal penalties for violation of the ITAR provisions, such as civil sanctions.

clear. The Court has given little guidance concerning the meaning of the operative term. In *Ohralik v. Ohio State Bar Ass'n*, 436 U.S. 447, 455–456 (1978), the Court indicated that “commercial speech” is “speech proposing a commercial transaction.” *See also Virginia Pharmacy Board, supra*. In *Central Hudson Gas*, by contrast, the Court described “commercial speech” as “expression related solely to the economic interests of the speaker and its audience.” 447 U.S. at 561. This characterization prompted a separate opinion from Justice Stevens, joined by Justice Brennan, suggesting that such a definition was far too broad: “Neither a labor leader’s exhortation to strike, nor an economist’s dissertation on the money supply, should receive any lesser protection because the subject matter concerns only the economic interests of the audience. Nor should the economic motivation of a speaker qualify his constitutional protection; even Shakespeare may have been motivated by the prospect of pecuniary reward.” *Id.* at 579–80.

The contours of the “commercial speech” concept are suggested by the facts of the cases that have recognized the commercial speech doctrine. As we have said, speech that promotes a commercial transaction falls within the category. *See id.* (advertisements promoting purchase of utility services and sales of electricity); *Virginia State Bd., supra* (advertisements for pharmaceutical products); *Linmark Associates, supra* (advertisements for real estate); *Friedman v. Rogers, supra* (use of trade name by optometrists). Thus far, the characterization as “commercial speech” has been largely confined to speech that merely promotes the sale or purchase of a product or service; in no case has it been applied to nonpromotional material simply because the speaker or writer is motivated by an economic interest, or because he is selling the information for a profit. We do not believe that the Court would hold that the transmission of technical data is “commercial speech” merely because the exporter charges a fee for its disclosure. Such a holding would prove far too much. It would sweep a broad range of fully protected expression into the commercial speech category. Writers of all varieties—political, literary, scientific, philosophical—often charge a fee for the books or articles they produce. There is no authority for the proposition that, simply by virtue of the fact that the documents are transferred for a fee, they are not protected by the First Amendment.

On the other hand, as we have suggested, the dissemination of technical data for the purpose of promoting the sale of a defense article or service would appear to be “commercial speech,” and the constitutional barriers to prior restraints may well have a diminished applicability to the dissemination of technical data in that context. As applied to such speech, the ITAR may well be constitutional, given the substantial governmental interest in suppressing the technical data and the qualified nature of the First Amendment protection that is accorded to promotional materials.

(3) *Transactions in which an exporter, unconnected with any foreign enterprise, disseminates technical data knowing or having reason to know that the data may be taken abroad and used there in the manufacture or use of arms.* Read in light of the relevant exemptions and definitions, the revised technical data provisions can be applied to any person who proposes to disseminate technical data in circumstances in which he knows or has reason to know that the information will be transmitted or taken abroad and used in the manufacture or use of arms. This coverage is so broad that the revised provisions could be applied in a number of factual settings to persons who are not directly connected or concerned in any way with any foreign conduct carrying dangerous potential for the United States. They could be applied, for example, to communications of unclassified information by a technical lecturer at a university or to the conversation of a United States engineer who meets with foreign friends at home to discuss matters of theoretical interest.

On the basis of the *Edler* decision, we believe that the technical data provisions may be applied constitutionally to persons or firms who combine (with the requisite *scienter*) with foreign enterprises to assist them in the development of sensitive technological capacities. In the absence of special circumstances,⁸ however, there is a critical constitutional difference between direct and immediate involvement in potentially dangerous foreign conduct, as in *Edler*, and the speech of the lecturer or the engineer in the examples given above. The difference is a factual one—the difference between conspiracy and assembly, incitement and informing—but it is no less important for constitutional purposes. See *Whitney v. California*, 274 U.S. 357, 376–77 (1927) (Brandeis, J., concurring). On the far side of that critical line, speech is not protected when it is brigaded with conduct; on the near side, it is at least arguably protected. Speech does not lose its protected character solely because the circumstances of the case give rise to a reasonable fear that persons other than the speaker may be moved or enabled by the speech to do dangerous things at remote times and places. See *Brandenburg v. Ohio*, 395 U.S. 444 (1969).⁹ Finally, if speech is arguably protected by the First Amendment, it may not be subjected to prior restraint except in the most extraordinary cases. Prior restraint against arguably protected speech is presumptively unconstitutional. See *Pittsburgh Press Co. v. Pittsburgh Comm’n on Human Relations*, *supra*.

⁸Special circumstances would include a grave and immediate threat to national security, as where important military information is being communicated to an adversary for current use against the United States. See *New York Times v. United States*, 403 U.S. 713 (1971).

⁹In *Brandenburg*, the Court held that speech would not be protected if it was both “directed to inciting or producing imminent lawless action” and “likely to incite or produce such action.” 395 U.S. at 447. The “directed to inciting” language at least arguably requires a showing of intent. Accordingly, when intent is absent, speech is—again at least arguably—protected by the First Amendment and may not, therefore, be suppressed by means of a prior restraint. A different conclusion may be appropriate, however, if very grave harm would definitely result from the disclosure. See *New York Times v. United States*, *supra*.

In accordance with these principles, we conclude that, in general, the revised technical data provisions cannot constitutionally be applied to the dissemination of technical data by persons having no direct connection with foreign conduct in settings in which there is no more than belief or a reasonable basis for believing (1) that a foreign national may take the technical data abroad and (2) that the data could be used by someone there in the manufacture or use of items on the Munitions List.¹⁰ In the absence of special circumstances that would justify prior restraint, such speech is arguably protected and, as a general rule, cannot be subjected constitutionally to the revised licensing requirement.

III. Conclusion and Recommendation

We have concluded that the revised technical data provisions can have constitutional and unconstitutional applications. As a matter of constitutional doctrine, that conclusion would require a court to consider whether the provisions are so substantially overbroad that they are void and unenforceable in all their applications. *See Broadrick v. Oklahoma*, 413 U.S. 601 (1973). For the present, however, we will forgo that inquiry in favor of three more pragmatic considerations.

First, *Edler* itself demonstrates that the problems presented by facial overbreadth do not necessarily prevent the enforcement of a licensing requirement in cases in which such a requirement can otherwise be constitutionally enforced. The *Edler* court saw its task as one of saving a necessary system of regulation, and it therefore chose to “construe” the statute and the applicable regulations narrowly to avoid the overbreadth problem and to preserve the possibility of enforcing the system against a criminal defendant (*Edler*) whose “speech” may not have been constitutionally protected. That approach was consistent with the approach that the Supreme Court itself has taken in some First Amendment cases. *See Civil Service Commission v. Letter Carriers*, 413 U.S. 548 (1972). It is an approach that may be taken when new cases arise under the revised technical data provisions.

Second, there is no absolute guarantee that other courts will be as concerned with saving the regulations as the *Edler* court was. The decision whether to enforce the overbreadth doctrine or to save the regulation through narrow “construction” is in part a matter of judicial discretion; and we cannot exclude the possibility that a court would

¹⁰ As *Edler* suggests, a different conclusion may be appropriate if the data have only military applications, or if the defendant knows such an application is intended. Even in such contexts, however, there may be situations in which the First Amendment bars a prior restraint consider, for example, a lecture on technical data having exclusively military uses when nationals of American allies are in the audience. We do not, however, conclude that the ITAR is unconstitutional with respect to all transactions falling within this category; we merely suggest it has a number of unconstitutional applications.

hold the technical data provisions substantially overbroad, and therefore void.

For obvious reasons, the best legal solution for the overbreadth problem is for the Department of State, not the courts, to narrow the regulations. In our judgment, the regulations should be narrowed to make it less likely that they will apply, or be seen to apply, to protected speech falling within the general category described in part 3 of section II above. We would respectfully recommend that an effort be undertaken along that line.¹¹

THEODORE B. OLSON
Assistant Attorney General
Office of Legal Counsel

¹¹ We also recommend the legislative changes referred to in note 7, *supra*.

EXHIBIT 8

Constitutionality of Proposed Revisions of the Export Administration Regulations

Proposed revisions of the Export Administration Regulations dealing with the export of technical data to foreign nationals apply a prior restraint, in the form of a licensing requirement, to a wide variety of speech protected by the First Amendment. There is thus a considerable likelihood that in their current form the regulations would be invalidated as unconstitutionally overbroad. The regulations would also be vulnerable to constitutional attack on grounds of vagueness. If the regulations were cast not as a licensing scheme but as a form of subsequent punishment, they could cover a far broader range of conduct.

A licensing system is likely to be held constitutional only if it applies narrowly to exports which are likely to produce grave harm under the test set forth in *New York Times Co. v. United States*, 403, U.S. 713 (1971).

July 28, 1981

MEMORANDUM OPINION FOR THE DIRECTOR, CAPITAL GOODS PRODUCTION MATERIALS DIVISION, DEPARTMENT OF COMMERCE

This will respond to your request for the views of this Office on the constitutional issues raised by your draft revision of Part 379 of the Export Administration Regulations. Those regulations clarify the circumstances in which a license is required for the export of technical data to foreign nationals. We believe that the regulations, as currently drafted, have a number of unconstitutional applications, and that they should therefore be substantially revised in order to meet the constitutional objections. In the discussion below, we offer a general statement of our reasoning, together with some suggestions for possible revision.

I. Background

The general purpose of the regulations is to require a license before the "export" of "technical data," subject to two exceptions discussed below. Under the regulations, technical data is defined as "information and know-how of any kind that can be used, or adapted for use, in the design, production, manufacture, repair, overhaul, processing, engineering, development, operation, maintenance, or reconstruction of commodities." The term "commodity" encompasses a wide range of articles compiled on the Commodities Control List. Many of the articles fall generally in the broad category of "high technology" items, including,

but not limited to, items subject to direct use for military purposes. However, the definition of commodities also embraces items with only indirect military application. An “export” is defined as an actual shipment or transmission of technical data out of the United States; any release of technical data in the United States with knowledge or intent that the data will be shipped or transmitted from the United States to a foreign country; and any release of technical data of United States origin in a foreign country.

Under the regulations, a critical distinction is made between “basic research”—research “directed toward an increase in knowledge”—and “applied research”—research “directed toward the practical application of knowledge.” In addition, “development” is defined as the systematic use of knowledge directed toward the design and production of useful prototypes, materials, devices, systems, methods, or processes.

The regulations grant a general license for two broad categories of technical data. The first category provides a general license applicable to all destinations and includes three subcategories, of which the first consists of data “made generally available to the public” through release at conferences that are open to the public in the sense that the general public or a range of qualified participants is eligible to attend. This license appears designed to cover conferences in which the information will not be closely held because of the generally open nature of the proceedings. The second subcategory consists of exports resulting from “basic [scientific] research,” but “applied research” is specifically excluded from this license. The third consists of data “released through formalized classroom instruction . . . at commercial, academic, government or private institutions,” provided that the instruction does not give access to applied research or development activities.

The second broad category provides a general license to a limited number of countries for two subcategories of technical data. The first consists of data in such forms as manuals or instruction books, provided that they are sent as part of a transaction directly related to commodities licensed for export and that they are not directly related to the production of commodities wholly or in part. The second subcategory includes technical data supporting a bid, lease, or offer to sell.

For all other exports of technical data, a license is required.

II. Discussion

The Export Administration Regulations represent an effort to serve the legitimate interests of the United States in controlling the dissemination of information to foreign countries, especially when the result of such dissemination may be the development of military equipment. The courts, however, have been almost invariably unwilling to uphold licensing schemes that require government approval before particular information may be disclosed. Such schemes amount to “prior re-

straints,” which are presumed invalid and subject to an exceptional burden of justification. *See New York Times Co. v. United States*, 403 U.S. 713 (1971). The courts have never held that the technical and scientific materials involved here—which, to be sure, do not contain political speech—are entitled to less than full protection under the First Amendment. In order to ensure that the regulations at issue here will survive judicial scrutiny under the First Amendment, we believe that it will be necessary to revise them and thus to guarantee that the legitimate interests that they attempt to promote will in fact be served if the regulations are challenged in court.

In a recent memorandum, this Office commented on the constitutional issues raised by a revision of the “technical data” provisions of the International Traffic in Arms Regulations (ITAR). *See Memorandum Opinion of July 1, 1981, from Theodore B. Olson, Assistant Attorney General, Office of Legal Counsel, for the Office of Munitions Control, Department of State.*^{*} In that memorandum, we divided the technical data provisions of the ITAR into three general categories, applying a separate First Amendment analysis to each. The first category included transactions involving arrangements entered into by exporters to assist foreign enterprises in the acquisition or use of technology. Following the decision in *United States v. Edler Industries, Inc.*, 579 F.2d 516 (9th Cir. 1978), we concluded that technical data exported during the course of such transactions fell into the same general category as communications made during the course of a criminal conspiracy. The courts treat such communications not as speech protected from prior restraint, but as an integral part of conduct that the government has a right to prevent. *See Ohralik v. Ohio State Bar Ass’n*, 436 U.S. 447, 456 (1978), and cases cited. We concluded, therefore, that technical data transmitted during the course of such transactions could constitutionally be subjected to a licensing requirement.

The second category consisted of technical data divulged for the purpose of promoting or proposing the sale of technical data or items on the munitions list. We concluded that this form of “commercial speech” would probably not be held subject to the prior restraint doctrine in light of the lower level of protection sometimes accorded to that speech and the substantial government interests at stake. *See Central Hudson Gas & Elec. v. Public Service Comm’n*, 447 U.S. 557 (1980).

The third category consisted of technical data disseminated by an exporter who is unconnected with any foreign enterprise, but who knows or has reason to know that the data may be taken abroad and used there in the manufacture or use of arms. Speech in this category, we concluded, would generally be protected from prior restraint. The

^{*} Note: The July 1, 1981, Memorandum Opinion is reprinted in this volume, at p. 206, *supra*. Ed.

Court has made clear that the First Amendment protects the right of Americans to communicate with foreigners, even if the foreigners are citizens of adversaries of the United States. *See Lamont v. Postmaster General*, 381 U.S. 301 (1965); *see also Kleindienst v. Mandel*, 408 U.S. 753 (1972).¹ The Court has also made clear that a prior restraint can be imposed only in the most compelling circumstances. *See New York Times Co. v. United States*, 403 U.S. 713 (1971). In the absence of such circumstances—such as a grave and immediate threat to national security, as where important military information is being communicated to an adversary for current use against the United States—speech falling in this category is protected from prior restraint. *See id.*

We believe that this general framework is the proper one from which to analyze the restrictions at issue here. Applying that framework, it is apparent that the revised regulations apply a prior restraint, in the form of a licensing requirement, to a wide variety of protected speech falling in the third category described in our memorandum on the ITAR. For example, scientists and researchers must obtain a license for exports of technical data resulting from applied research. The results of such research are, however, entitled to full protection under the First Amendment. Similarly, the regulations subject university instruction to a licensing requirement if the instruction includes applied research or development activities. This requirement applies a prior restraint to protected speech and is thus impermissible except in the most compelling circumstances. For example, we do not believe that the courts would uphold a requirement that a professor obtain a license before “releasing” information to foreign students simply because the information may be used in the overhaul of certain kinds of computer chips. The same considerations suggest that an American scientist could not be barred in advance from informing his colleagues, some of whom are foreign nationals, of the results of an experiment that could help produce some other high technology item. Other examples could readily be imagined. In more general terms, the regulations cover a wide variety of speech that is constitutionally protected. We believe that they should therefore be substantially narrowed. Indeed, the range of impermissible applications is sufficiently great, and the number of permissible applications so comparatively small, that there is a considerable likelihood that in their current form the regulations would be invalidated as substantially overbroad under *Broaderick v. Oklahoma*, 413 U.S. 601 (1973).

We note in addition that the regulations are vulnerable to claims of vagueness in two critical respects. First, the distinction between “applied research” and “basic research” seems to be too thin to support the

¹ The Court has apparently not authoritatively determined whether and to what extent Americans have First Amendment rights while travelling abroad. *See Haig v. Agee*, 453 U.S. 280 (1981) (assuming such rights *arguendo*).

conclusion that "applied research" can in all contexts be subjected to the licensing requirement. Second, the definition of an export as a "release of technical data . . . with knowledge or intent that the data will be . . . transmitted from the United States to a foreign country" is highly ambiguous. In order to be subject to the licensing requirement, must the speaker know with a high degree of certainty that the data will be so transmitted? Or, as we have been told informally, is it sufficient if he knows that foreign nationals are among his audience? If the first interpretation is adopted, the regulations will of course be substantially more narrow.

While we are not at this stage prepared to describe in detail what materials may, consistent with the First Amendment, be covered by the regulations, we would like to conclude with some general observations. First, the legal difficulties in this context arise largely because of the profound constitutional hostility to prior restraints. If the regulations were cast, not as a licensing scheme, but as a form of subsequent punishment, they could cover a far broader range of conduct. Under *Brandenburg v. Ohio*, 395 U.S. 444, 447 (1969), the government may punish speech that is both "directed to inciting or producing imminent lawless action" and "likely to . . . produce such action" (footnote omitted). Similar considerations may justify subsequent punishment for the export of technical data in circumstances in which the exporter knows or intends that the result will likely be harmful to the national security interests of the United States. In order to implement such a scheme of subsequent punishment, persons planning to "export" might be given an opportunity, but not required, to seek advice from the Secretary of Commerce as to whether the particular disclosure is prohibited by law.

Second, if a licensing system is to be retained, the constitutional prohibition against prior restraint suggests that it may be applied only to exports that are very likely to produce grave harm. See *New York Times Co. v. United States*, *supra*. Under this rationale it may be permissible to require a license before a person may disclose (with the requisite *scienter*) technical data having direct military applications to an adversary of the United States. Apart from this limited category, we believe that the prior restraint doctrine bars a licensing requirement.

As noted above, these comments are directed to the current version of your regulations. We will be pleased to provide further comments or assistance with respect to any future revisions.

THEODORE B. OLSON
Assistant Attorney General
Office of Legal Counsel

EXHIBIT 9



U.S. Department of Justice
Office of Legal Counsel

Office of the
Deputy Assistant Attorney General

Washington, D.C. 20530

JUL 5 - 1984

MEMORANDUM FOR DAVIS R. ROBINSON
LEGAL ADVISER
DEPARTMENT OF STATE

Re: Revised Proposed International Traffic in
Arms Regulations (ITAR)

This responds to a memorandum of June 5, 1984, from Mr. Cummings of your Office, requesting the views of this Office on a proposed revision of the International Traffic in Arms Regulations (ITAR), recently prepared by the Department of State (hereinafter "current draft"). This Office has previously provided extensive comments on an earlier proposed revision of the ITAR (hereinafter "prior draft"). 1/ See Memorandum for William B. Robinson, Office of Munitions Control, Department of State, from Theodore B. Olson, Assistant Attorney General, Office of Legal Counsel (July 1, 1981) (hereinafter "1981 ITAR

1/ This Office first addressed constitutional issues related to the ITAR in 1978 in a memorandum for Dr. Frank Press, the Science Adviser to President Carter. That opinion considered the constitutionality of the restrictions on the dissemination of cryptographic information developed by scientists and mathematicians in the private sector independent of government supervision or support. We concluded that the ITAR's prohibition of disclosure of these "public" cryptographic ideas and information amounted to an unconstitutional prior restraint. See Memorandum for Dr. Frank Press, Science Adviser to the President, from John M. Harmon, Assistant Attorney General, Office of Legal Counsel (May 11, 1978) (attached).

Memorandum"). 2/ For reasons set forth in detail below, we believe that the current draft is an improvement over the prior draft, but that the application of the ITAR to a significant class of conduct continues to raise serious constitutional questions, which should be resolved prior to promulgation of the revised ITAR.

I. BACKGROUND

In our 1981 memorandum, we discussed primarily the restrictions on, and the exemptions allowed for, the "export" of "technical data." Under the ITAR, the "export" of "technical data" is subject to a licensing requirement unless it falls within one of the exemptions. We concluded that the prior draft of the ITAR had a number of unconstitutional applications, specifically with regard to transactions in which an exporter, unconnected with any foreign enterprise, disseminated technical data knowing or having reason to know that the data may be taken abroad and used there in the manufacture or use of arms. We noted that the coverage of the technical data provisions was so broad that they

could be applied in a number of factual settings to persons who are not directly connected or concerned in any way with any foreign conduct carrying dangerous potential for the United States. They could be applied, for example, to communications of unclassified information by a technical

2/ In 1981, we also issued an opinion which addressed the constitutionality of proposed regulations under the Export Administration Act (EAA) regarding the export of technical data relating to items on the Department of Commerce's Commodities Control List. These regulations proposed generally the same definitions, prohibitions, and licensing requirements with respect to technical data associated with commodities as the ITAR proposed for technical data associated with munitions. We concluded that the proposed EAA regulations also amounted to an unconstitutional prior restraint on the disclosure of a wide variety of protected speech. See Memorandum for Henry D. Mitman, Director, Capital Goods Production Materials Divisions, Department of Commerce, from Theodore B. Olson, Assistant Attorney General, Office of Legal Counsel (July 28, 1981) (attached).

lecturer at a university or to the conversation of a United States engineer who meets with foreign friends at home to discuss matters of theoretical interest.

1981 ITAR Memorandum at 13.

Relying on the decision in United States v. Edler Industries, Inc., 579 F.2d 516 (9th Cir. 1978), we concluded in 1981 that the technical data provisions could be constitutionally applied to persons or firms who assisted foreign enterprises in the development of sensitive technological capacities. We also concluded, however, that in the absence of special circumstances, such as a grave and immediate threat to national security, the difference between direct and immediate involvement in potentially dangerous conduct, such as in the Edler case, and the speech of a lecturer or engineer in the hypothetical posed above, could be critical for constitutional purposes. Thus, the technical data provisions could not constitutionally be applied to the dissemination of technical data by persons having no direct connection with foreign conduct in settings in which there is no more than a belief or a reasonable basis for believing: (1) that a foreign national may take technical data abroad; and (2) that the data could be used by someone there in the manufacture or use of items on the controlled munitions list. In the absence of special circumstances that would justify a prior restraint on such speech, the speech was presumptively protected and therefore could not constitutionally be subjected to a licensing requirement.

The 1981 ITAR Memorandum did not purport to determine the constitutionality of all possible applications of the ITAR. We merely advised that there were a number of unconstitutional applications which would make the regulations overbroad. We suggested that the regulations be narrowed to make it less likely that they would apply, or might be thought by a court to apply, to protected speech.

II. SUBSEQUENT LEGAL DEVELOPMENTS

Since we wrote our 1981 ITAR Memorandum, the Supreme Court has decided two commercial speech cases. In both cases, the Court has continued the extent of protection of commercial speech recognized in the earlier cases, upon which our previous memorandum relied. The details of the two more recent cases are not relevant to our analysis here, but it is

important to note that, in our judgment, the constitutional principles upon which we relied remain intact. 3/

III. DISCUSSION

The current draft of the ITAR circulated by your Office was apparently intended to remedy the constitutional defects

3/ In Metromedia, Inc. v. San Diego, 453 U.S. 490 (1981) (plurality opinion), the Court considered a city ordinance which permitted onsite commercial advertising but prohibited offsite commercial advertising and noncommercial advertising with limited exceptions. The plurality opinion concluded that the ordinance was constitutional as applied to commercial speech because it satisfied the standards of Central Hudson Gas & Electric Corp. v. Public Service Comm'n, 447 U.S. 557 (1981), upon which we relied in our prior opinion. The substantial government interests in improved traffic safety and appearance of the city were directly served by the ordinance, which was no broader than necessary to accomplish those ends. (The ban was invalidated as applied to noncommercial speech, however, because the Government's asserted interests were insufficient to justify the ban, given that commercial advertising was permitted.) In Bolger v. Youngs Drug Products Corp., 103 S. Ct. 2875 (1983), the Court struck down a federal statute which prohibited unsolicited mailing of contraceptive advertisements. The Court held that the statute was an unconstitutional restriction on commercial speech because the Government's interests in shielding recipients from unwanted mail which they might find offensive and aiding parents in controlling the information which their children received about birth control were insufficient to overcome the protection afforded to speech that was truthful and related to activity protected from unwanted state interference and also to important social issues. City of Los Angeles v. Taxpayers for Vincent, No. 82-975, 52 U.S.L.W. 4594 (U.S. May 15, 1984), is a sort of sequel to Metromedia, although it is not a commercial speech case. In Taxpayers, the Court upheld a city ordinance which prohibited the posting of signs on public property. The Court held that the content-neutral prohibition was justified by the city's substantial esthetic interests, even as applied to signs which carried political messages. Of course, the ordinance was directed against--and prohibited--only the use of the signs. Speech itself was not regulated and could be continued to be conveyed on public property by a speaker or distributor of leaflets.

existing in the prior draft. The summary of the current draft notes that the list of exemptions from the licensing requirement of the ITAR was one of the provisions which received the most comments and that concerns were expressed about the relationship between that licensing requirement and the First Amendment. The summary states that the revision "seeks to reflect these concerns, and certain new exemptions are provided." Prior draft at p. 10. We have examined the new exemptions as well as the revised definitions of "export" and "technical data," and we offer the following comments. For convenience, the relevant provisions of the prior and current drafts are set out in full as an appendix to this opinion.

A. "EXPORT"

The definition of export with regard to technical data has been changed. ^{4/} The prior draft described four general ways in which technical data could be exported:

- (1) sending, transmitting, or taking defense articles and defense services, including technical data, out of the United States in any manner, see § 121.34(a)(1);
- (2) the disclosure to a foreign national of technical data relating to significant military equipment in the United States; see § 121.34(b), first sentence 5/;

^{4/} The definitions of export in the current draft with regard to "defense articles" and "defense services" seem to be substantively unchanged from the prior draft, at least for purposes of constitutional evaluation. These provisions were not within the scope of our 1981 ITAR Memorandum, and they are not relevant here.

^{5/} This sentence describes a narrower category than category (4), see p. 6, infra, because it applies only to technical data relating to significant military equipment, not all technical data, but this category is also broader than category (4) because, as applied to technical data relating to significant military equipment, this provision does not require that the transferor know or have reason to know that the technical data will be disclosed outside the United States.

(3) the disclosure of technical data to a foreign national abroad, see id., second sentence 6/; and

(4) the disclosure of technical data to a foreign national in the United States when the transferor knows or has reason to know that the disclosed technical data will be disclosed outside the United States, see id., third sentence. 7/

Travel abroad by a U.S. national or permanent resident with personal knowledge of technical data was excluded from the definition of export. See id., fourth sentence.

Under the current draft, these four categories appear to be consolidated into two:

(1) sending or taking technical data outside the United States in any manner except for travel by a person with personal knowledge of technical data, see § 121.20(c); and

(2) disclosing or transferring technical data to a foreign person, whether in the United States or abroad, unless an exemption is applicable. See § 121.20(d).

It appears to us that the first category of export under both the prior and current drafts is substantively identical, although in slightly different form. Under the prior draft, travel abroad was also exempted, although the exemption was contained in the subsection relating to disclosure and did not specifically refer to sending or taking technical data out of the United States.

The difference between the two drafts is that the second, third, and fourth categories of exports in the prior draft have

6/ As drafted, the first sentence of § 121.34(b) referred also to disclosures of technical data relating to significant military equipment abroad. Given that this second sentence refers to disclosure of any technical data abroad, the reference in the first sentence to disclosure abroad of technical data relating to significant military equipment seems superfluous.

7/ This provision seems duplicative of § 121.34(a)(2), which refers to the transfer of technical data to a foreign national in the United States in circumstances in which the transferor knows or has reason to know that the technical data will be sent, transmitted, or taken out of the United States.

been condensed into the second category in the current draft. On its face, and without regard to the exemptions, the scope of coverage of the current draft is broader because it applies to all disclosures and transfers of technical data to a foreign person in the United States and abroad, unless exempted, whereas the prior draft seemed to require that the transferor know or have reason to know that technical data other than that relating to significant military equipment would be disclosed outside the United States. Thus, whether the coverage of the current draft is narrower for constitutional purposes than the prior draft depends on the scope of the exemptions provided in the current draft. We examine those exemptions in detail below, although we will discuss the definition of "technical data" first in order to complete the background for our inquiry.

B. "TECHNICAL DATA"

Both the prior and the current drafts describe generally three types of technical data. Two are substantially identical:

(1) classified information relating to defense articles and defense services, see § 121.315(b) (prior draft) and § 121.30(a) (current draft); and

(2) information covered by a patent secrecy order, see § 121.315(c) (prior draft), or an invention secrecy order, see § 121.30(b) (current draft).

The third category is described in the prior draft as "unclassified information not in the public domain relating directly to" various categories of information. See § 121.315(a). The current draft is phrased in terms of "information which is not classified pursuant to U.S. laws and regulations and which is directly related to" generally the same kinds of information. See § 121.30(c). Essentially, this information relates to the "design, engineering, development, production, processing, manufacture, operation, overhaul, repair, maintenance, or reconstruction of defense articles." The current draft specifically includes "information which advances the state of the art of articles on the U.S. Munitions List." See § 121.30(c). 8/

8/ The prior draft differs by referring to information which is related to "training" in the operation, use, overhaul, repair, or maintenance of an article. This difference does not appear to be a substantive change. The prior draft also included "performance of a defense service" within the definition of technical data. Performance of a defense service is now specifically covered in § 121.18.

Two changes have been made in the definition of technical data in the current draft, which specifically excludes information in the "public domain" and "general mathematical and engineering information which is only and [sic] indirectly useful in the defense field." Information in the public domain is defined to include information which is published and generally accessible or available to the public at newsstands and bookstores, through certain subscriptions, through certain mailing privileges, and at public libraries. In the prior draft, these same types of information were exempt by general exemptions from the licensing requirement, rather than through exclusions from the definition of technical data. See § 125.11(a)(1) and (10). Thus, although the definitions of technical data in the prior and current drafts differ because of the exclusion in the current draft of information in the public domain and general mathematical or engineering information, we do not believe that this difference amounts to a substantive change in the coverage of the regulations. If the scope of the application of the licensing scheme under the current draft is narrower, it would be only if the scope of the exemptions were broader. We turn therefore to an examination of the exemptions.

C. EXEMPTIONS

The prior draft contained ten exemptions. The current draft contains thirteen. Of the ten exemptions provided in the prior draft, the first related to technical data which was published or otherwise generally available to the public. The last related to "information which was not designed or intended to be used, or which could not reasonably be expected to be used, in direct application in the design, production, [etc.], of defense articles (for example, general mathematical, engineering, or statistical information not purporting to have or not reasonably expected to be given direct application to defense articles)." As noted above, these categories of information are generally covered in the current draft by exclusions from the definition of technical data. Thus, there are eight exemptions contained in the prior draft which must be compared to the current draft, and four additional exemptions provided in the current draft to examine.

Six of the exemptions appear to be substantively identical to, if not verbatim repetitions from, the prior draft. These provisions are identified in the footnote below and are not

relevant to our discussion. 9/ The two remaining exemptions contained in the prior draft have been narrowed in the current

<u>9/ Category of Exemption</u>	<u>Prior Draft</u>	<u>Current Draft</u>
Export in furtherance of a manufacturing license or technical assistance agreement approved by the Department of State.	§ 125.11(a)(3).	§ 125.4(b)(2)
Export in furtherance of a contract between the exporter and the U.S. Government which provides for the export of certain technical data.	§ 125.11(a)(4)	§ 125.4(b)(3)
Export of manuals and aids relating to lawfully exported articles to the same recipient.	§ 125.11(a)(5)	§ 125.4(b)(5)
Export of additional copies or certain revised copies of technical data previously exported or authorized to be exported to the same recipient.	§ 125.11(a)(6)	§ 125.4(b)(4)
Export of data relating to firearms and ammunition not in excess of .50 caliber.	§ 125.11(a)(7)	§ 125.4(b)(6)
Export of data directly relating to classified information previously exported to the same recipient.	§ 125.11(a)(9)	§ 125.4(b)(8)

draft. The revision does not appear to raise any constitutional issues. 10/

The current draft contains five new exemptions. (For convenience, we will refer to these five exemptions by the subsection number of § 125.4(b) of the current draft.) Two of the exemptions, subsections (1) and (11), do not alleviate the effect of the licensing requirement as a prior restraint on the export of technical data as defined in the regulations. Subsection (1) exempts information which relates to defense articles but does not qualify as technical data pursuant to the definition in § 121.30. Because we are concerned in this memorandum only with information which is defined as technical data and subject to export restrictions because of that definition, subsection (1), although useful for purposes of clarity,

10/ The prior draft contained an exemption, § 125.11(a)(2), for information approved for public release by any U.S. Government department or agency having authority to classify information and material which did not disclose details relating to articles on the munitions list. The corresponding provision in the current draft, § 125.4(b)(13), exempts information approved for public release by the federal department or agency which originated or developed the information. We understand that the purpose of this change was to make clear that only the department or agency which generated the information could confer the exemption for export by prior approval of the information for public release. This change was designed to prevent a situation in which the action by one agency of releasing to the public information of another agency, even if not authorized to do so, would have the consequence of not only putting that information into the public domain but also triggering the exemption and thereby allowing export of that information without a license. We must caution, however, that we are not sure that this revision will have the intended effect. If the information is publicly released by any agency of the Government, we do not know how that information could be "recaptured" by the Government. Once the information is in the public domain, we cannot conceive of circumstances in which its export could be constitutionally restricted.

The second change relates to technical data which is being returned to the original source of import. In the prior draft, the exemption applied to all technical data. See § 125.11(a)(8). The current draft is limited to information which is not classified technical data. See § 125.4(b)(7). We understand that the purpose of this change is to withdraw the exemption allowed under the prior version for the export of classified information without a license.

does not affect our consideration of the scope of the prohibition of the export of technical data without a license or without an exemption from the licensing requirement.

Subsection (11) exempts the export of technical data pursuant to an arrangement with the Department of Defense or NASA which requires such exports if the exporter has been granted an exemption in writing from the licensing provisions by the Office of Munitions Control. In our view, the requirement of obtaining an exemption in writing is no different for purposes of First Amendment analysis from the requirement of obtaining the license itself. Both operate as a prior restraint, and both can be subject to the discretion of the executive officer from whom each must be sought. ^{11/} We do not believe, therefore, that this exemption significantly affects the scope of the licensing requirement under the ITAR.

Two of the new exemptions do provide greater freedom from prior restraint on the export of technical data, although they apply only in narrow factual circumstances. Subsection (9) exempts an export by a U.S. corporation to a U.S. person employed by that corporation overseas, subject to two conditions: that the information must be used solely by U.S. persons and the U.S. person must be directly employed by the U.S. corporation and not by a foreign subsidiary. The exemption is further subject to the limitations found in § 125.1(b) of the current draft, which precludes use of the license for export of technical data for foreign production purposes or technical assistance unless approved in advance by the Department of State.

Subsection (12) exempts any exports specifically exempted under Part 126 of the subchapter of the ITAR, which includes shipments by or for federal agencies, certain exemptions for unclassified technical data exported to and for use in Canada, and certain exports under the foreign military sales program. With the exception of the exemption for exports to Canada, these exemptions do not significantly narrow the scope of the licensing requirement as applied to private persons.

By expanding the exemptions to the licensing requirement, these two exemptions, subsections (9) and (12), do improve the constitutional status of the ITAR, which, as our prior

^{11/} We understand from Mr. Cummings that this written consent may actually take the form of a license or, for reasons relating to customs or possibly other laws, it may take the form of a letter granting consent.

opinion concluded, suffered from overbreadth because of the number of unconstitutional applications which we believed the ITAR to have. To the extent that the exemptions are expanded, the overbreadth is reduced. Our concern, however, is that neither of these exemptions addresses the specific examples of unconstitutional prior restraint identified in our prior opinion, that is, "communications of unclassified information by a technical lecturer at a university or to the conversation of a United States engineer who meets with foreign friends at home to discuss matters of theoretical interest." See 1981 ITAR Memorandum at 13.

The remaining exemption, subsection (10), appears to be an effort to address these types of situations, although this exemption is also insufficient to eliminate the licensing requirement in the two specific factual settings posed in the hypothetical above, as well as other situations which may be easily suggested. Subsection (10) exempts disclosure of unclassified information by U.S. corporations or academic institutions to foreign persons who are their bona fide and full time regular employees 12/ if an employee's permanent abode is in the United States; an employee is not a national of a country to which exports are specifically prohibited by the ITAR 13/; and the corporation or institution informs that employee in writing that the technical data may not be transferred to other foreign persons without the written

12/ As we understand from Mr. Cummings, this exemption was intended to be exercised by the employment office of the corporation or the university, which would have the responsibility for informing its employees of the extent of their rights to disclosure to other employees without the prior written consent of the Office of Munitions Control.

13/ Pursuant to § 126.1 of the current draft, these countries are: Albania, Bulgaria, Cuba, Czechoslovakia, East Germany, Estonia, Hungary, Kampuchea, Latvia, Lithuania, North Korea, Outer Mongolia, Poland, Rumania, the Soviet Union, Vietnam, and any other country or area with respect to which the United States maintains an arms embargo or "whenever an export would not otherwise be in furtherance of world peace and the security and foreign policy of the United States." We assume that these other countries are publicly announced, from time to time, according to some objective criteria, so that their identity and the basis for the prohibition of exports to that country may be known to potential exporters.

consent of the Office of Munitions Control. Under this subsection, an exemption would be provided for full time, regular employees of a single corporation or university to discuss technical data among themselves. What is not exempt, however, without the prior written consent of the Office of Munitions Control, is a disclosure of the information by an employee of a corporation or university to a foreign national who is a part-time or temporary employee of that corporation or university; a full time employee of another corporation or university; another professional person attending a conference or a seminar at the corporation or university; a student; or a friend.

We recognize the attempt made to address the concerns raised in our prior opinion, and, as we stated with regard to the new exemptions provided in subsections (9) and (12), to the extent that subsection (10) constricts the area of application of the licensing requirement, the additional exemption reduces the area of potential unconstitutional application of that requirement. We have identified, however, a number of circumstances in which the prior written consent of the Office of Munitions Control would be required for disclosure of the technical data. As noted above, with regard to subsection (11), which requires the written consent of that Office for export of certain technical data pursuant to an arrangement with the Department of Defense or NASA, we do not believe that there is a constitutionally significant distinction between the requirement of obtaining prior written consent and obtaining a license. See note 11, supra. In some of these circumstances, as well as others, we believe that the ITAR may still be read to operate as a prior restraint on the speech of "persons having no direct connection with foreign conduct in settings in which there is no more than belief or a reasonable basis for believing (1) that a foreign national may take the technical data abroad and (2) that the data could be used by someone there in the manufacture or use of items on the Munitions List." 1981 ITAR Memorandum at 14. As we concluded in that memorandum, "[i]n the absence of special circumstances that would justify prior restraint, such speech is arguably protected and, as a general rule, cannot be subjected constitutionally to the . . . licensing requirement." Id.

We are aware of the case law interpreting 22 U.S.C. § 2778, the statutory authority for the ITAR, which requires a specific intent willfully to export particular goods on the Munitions List without a license. See, e.g., United States v. Hernandez, 662 F.2d 289, 292 (5th Cir. 1981) ("statute's requirement of willfulness connote[s] a voluntary and intentional violation

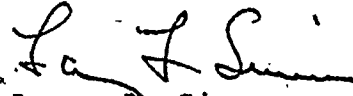
of a known legal duty," that is, "that the defendant knew that he was unlawfully exporting weapons on the Munitions List"); United States v. Beck, 615 F.2d 441, 449-50 (7th Cir. 1980) (conviction requires "proof that the defendants (1) exported or attempted to export (2) goods on the United States Munitions List (3) without first having obtained a license for the export (4) willfully"); and United States v. Wieschenberg, 604 F.2d 326, 331 (5th Cir. 1979) (to sustain a conviction for conspiracy to violate the statute, "government must prove that the defendants agreed to and specifically intended to export without a license particular property that is restricted by the Munitions List"). It may be that the standard of knowledge and intent that is imposed by these cases with regard to the export of defense articles might, as applied to technical data, be sufficient to broaden, in effect, the scope of the exemption under subsection (10) to the extent consistent with the constitutional standard articulated in our previous memorandum and reaffirmed here.

We remain of the opinion, however, that on their face, the ITAR still present some areas of potentially unconstitutional application, and, moreover, that we cannot be certain whether existing case law would be sufficient to narrow the range of application to a constitutionally sufficient extent. In any event, as we advised in our 1981 Memorandum with regard to the overbreadth present in the prior draft, we believe that "the best legal solution . . . is for the Department of State, not the courts, to narrow the regulations." See 1981 ITAR Memorandum at 15.

IV. CONCLUSION

We have carefully examined the definitions of "export" and of "technical data," as well as the exemptions provided from the licensing requirement, under the current draft of the ITAR, and we believe that the scope of the exemptions is broader, and the coverage of the licensing requirement therefore narrower, in at least three specific areas of importance to private persons: exports by disclosures to certain employees of U.S. corporations overseas (subsection (9)); certain exports to Canada (subsection (12)); and exports by disclosure of technical data by U.S. corporations and academic institutions to foreign nationals who are their full time, regular employees, subject to certain conditions (subsection (10)). Notwithstanding these additional exemptions, however, we have identified certain areas which still appear to us to

present sensitive constitutional issues. As we previously recommended, this remaining overbreadth should be eliminated by more narrowly drafted regulations.



Larry L. Simms
Deputy Assistant Attorney General
Office of Legal Counsel

Attachments:

Appendix of regulations
Memorandum of May 11, 1978, for Dr. Frank Press
Memorandum of July 28, 1981, for Henry D. Mitman

EXHIBIT 10

This web site was copied prior to January 20, 2005. It is now a Federal record managed by the National Archives and Records Administration. External links, forms, and search boxes may not function within this collection. [Learn more.](#) [\[hide\]](#)



1997 REPORT ON THE AVAILABILITY OF BOMBMAKING INFORMATION

PREPARED BY THE UNITED STATES DEPARTMENT OF JUSTICE
AS REQUIRED BY SECTION 709(a) IF THE
ANTITERRORISM AND EFFECTIVE DEATH PENALTY ACT OF 1996

SUBMITTED TO:

THE UNITED STATES HOUSE OF REPRESENTATIVES
AND THE UNITED STATES SENATE

APRIL 1997

TABLE OF CONTENTS

[INTRODUCTION AND SUMMARY](#)

[BACKGROUND](#)

- [I.](#) THE PUBLIC AVAILABILITY OF INFORMATION ON THE MANUFACTURE OF BOMBS, DESTRUCTIVE DEVICES, AND WEAPONS OF MASS DESTRUCTION
 - [A.](#) Books, Pamphlets and Other Printed Material
 - [B.](#) The Internet
 - [C.](#) Summary
- [II.](#) THE EXTENT TO WHICH PUBLISHED BOMBMAKING INFORMATION HAS FACILITATED THE MANUFACTURE AND USE OF EXPLOSIVES IN ACTS OF TERRORISM AND OTHER CRIMINAL ACTIVITY
- [III.](#) THE LIKELIHOOD THAT PUBLISHED BOMBMAKING INFORMATION WILL CONTINUE TO BE USED TO FACILITATE ACTS OF TERRORISM AND OTHER CRIMINAL ACTIVITY

IV. APPLICABILITY OF CURRENT FEDERAL LAW TO THE PUBLICATION AND DISSEMINATION OF BOMBMAKING INFORMATION

- A. Conspiracy
- B. Solicitation
- C. Aiding and Abetting
 - 1. 18 U.S.C. § 2
 - 2. AEDPA Section 323
- D. 18 U.S.C. § 231(a)(1)

V. THE NEED FOR ADDITIONAL LAWS RELATING TO THE DISSEMINATION OF BOMBMAKING INFORMATION

VI. CONSTITUTIONALITY OF RESTRICTING OR PENALIZING THE PUBLICATION OR DISSEMINATION OF BOMBMAKING INFORMATION

- A. First Amendment Principles
 - 1. Advocacy of Unlawful Action
 - 2. Disclosure or Publication of Lawfully Obtained Information
 - 3. "Speech Acts," such as Aiding and Abetting
- B. Application of First Amendment Principles To Dissemination of Bombmaking Information
 - 1. Dissemination with the "Intent" to Facilitate Unlawful Conduct
 - 2. Dissemination with the "Knowledge" that a Particular Recipient of the Information Intends to Use it in Furtherance of Unlawful Conduct
- C. Proposed Modification of the Feinstein Amendment

INTRODUCTION AND SUMMARY

In section 709(a) of the Antiterrorism and Effective Death Penalty Act of 1996 ["the AEDPA"], Pub. L. No. 104-132, 110 Stat. 1214, 1297 (1996), Congress provided that, in consultation with such other officials and individuals as she considers appropriate, the Attorney General shall conduct a study concerning --

(1) the extent to which there is available to the public material in any medium (including print, electronic, or film)

that provides instruction on how to make bombs, destructive devices, or weapons of mass destruction;

- (2) the extent to which information gained from such material has been used in incidents of domestic or international terrorism;
- (3) the likelihood that such information may be used in future incidents of terrorism;
- (4) the application of Federal laws in effect on the date of enactment of this Act to such material;
- (5) the need and utility, if any, for additional laws relating to such material; and
- (6) an assessment of the extent to which the first amendment protects such material and its private and commercial distribution.

Section 709(b) of the AEDPA, in turn, requires the Attorney General to submit to the Congress a report containing the results of the study, and to make that report available to the public.

Following enactment of the AEDPA, a committee was established within the Department of Justice ["the DOJ Committee"], comprised of departmental attorneys as well as law enforcement officials of the Federal Bureau of Investigation and the Treasury Department's Bureau of Alcohol, Tobacco and Firearms. The committee members divided responsibility for undertaking the tasks mandated by section 709. Some members canvassed reference sources, including the Internet, to determine the facility with which information relating to the manufacture of bombs, destructive devices and other weapons of mass destruction could be obtained. Criminal investigators reviewed their files to determine the extent to which such published information was likely to have been used by persons known to have manufactured bombs and destructive devices for criminal purposes. And legal experts within the Department of Justice reviewed extant federal criminal law and judicial precedent to assess the extent to which the dissemination of bombmaking information is now restricted by federal law, and the extent to which it may be restricted, consistent with constitutional principles. This Report summarizes the results of these efforts.

As explained in this Report, the DOJ committee has determined that anyone interested in manufacturing a bomb, dangerous weapon, or a weapon of mass destruction can easily obtain detailed instructions from readily accessible sources, such as legitimate reference books, the so-called underground press, and the Internet. Circumstantial evidence suggests that, in a number of crimes involving the employment of such weapons and devices, defendants have relied upon such material in manufacturing and using such items. Law enforcement agencies believe that, because the availability of bombmaking information is becoming increasingly widespread (over the Internet and from other sources), such published instructions will continue to play a significant role in aiding those intent upon committing future acts of terrorism and violence.

While current federal laws -- such as those prohibiting conspiracy, solicitation, aiding and abetting, providing material support for terrorist activities, and unlawfully furthering civil disorders -- may, in some instances, proscribe the dissemination of bombmaking information, no extant federal statute provides a satisfactory basis for prosecution in certain classes of cases that Senators Feinstein and Biden have identified as particularly troublesome. Senator Feinstein introduced legislation during the last Congress in an attempt to fill this gap. The Department of Justice agrees that it would be appropriate and beneficial to adopt further legislation to address this problem directly, if that can be accomplished in a manner that does not

impermissibly restrict the wholly legitimate publication and teaching of such information, or otherwise violate the First Amendment.

The First Amendment would impose substantial constraints on any attempt to proscribe indiscriminately the dissemination of bombmaking information. The government generally may not, except in rare circumstances, punish persons either for advocating lawless action or for disseminating truthful information -- including information that would be dangerous if used -- that such persons have obtained lawfully. However, the constitutional analysis is quite different where the government punishes speech that is an integral part of a transaction involving conduct the government otherwise is empowered to prohibit; such "speech acts" -- for instance, many cases of inchoate crimes such as aiding and abetting and conspiracy -- may be proscribed without much, if any, concern about the First Amendment, since it is merely incidental that such "conduct" takes the form of speech.

Accordingly, we have concluded that Senator Feinstein's proposal can withstand constitutional muster in most, if not all, of its possible applications, if such legislation is slightly modified in several respects that we propose at the conclusion of this Report. As modified, the proposed legislation would be likely to maximize the ability of the Federal Government -- consistent with free speech protections -- to reach cases where an individual disseminates information on how to manufacture or use explosives or weapons of mass destruction either (i) with the intent that the information be used to facilitate criminal conduct, or (ii) with the knowledge that a particular recipient of the information intends to use it in furtherance of criminal activity.

BACKGROUND

In order fully to understand the issues we have been asked to address, it is helpful first to describe the legislative proceedings that prompted enactment of section 709 of the AEDPA.

On May 11, 1995, less than one month after the Oklahoma City terrorist bombing, in testimony before the Subcommittee on Terrorism, Technology and Government Information of the Senate Judiciary Committee, Deputy Assistant Attorney General Robert Litt, of the Justice Department's Criminal Division, explained that "how to" guides for the manufacture of explosives are readily available on the Internet, in bookstores and even in public libraries¹. To illustrate the point, he observed that, according to a news article, only hours after the Oklahoma City bombing, someone posted on the Internet directions -- including a diagram -- explaining how to construct a bomb of the type that was used in that tragic act of terrorism. Another Internet posting offered not only information concerning how to build bombs, but also instructions as to how the device used in the Oklahoma City bombing could have been improved.

Mr. Litt explained that "expansion of the scope of federal criminal laws dealing with the violent, terrorist activity will permit the Department of Justice to prosecute those who engage in efforts to assist violence and terrorism over the Internet." Mr. Litt observed, however, that despite the dangers posed by the dissemination of such information and the callous disregard of human life shown by those who are responsible for such action, the First Amendment imposes significant constraints on the ability of the federal government to proscribe and penalize such activity.

On June 5, 1995, Senator Feinstein proposed an amendment to a bill (S. 735) that later became the AEDPA. 141 Cong. Rec. S7682 (daily ed. June 5, 1995). The purpose of the amendment was to address the problem of the increasingly widespread "distribution of bombmaking information for criminal purposes." *Id.* Following some debate in the Senate, Senator Feinstein's amendment was slightly modified, and the full Senate unanimously approved it by voice vote. *Id.* at S7686. The Senate passed S. 735 on June 7, 1995. 141

Cong. Rec. S7857 (daily ed.). As passed by the Senate, the Feinstein amendment would have amended 18 U.S.C. § 842 to add a new prohibition:

It shall be unlawful for any person to teach or demonstrate the making of explosive materials, or to distribute by any means information pertaining to, in whole or in part, the manufacture of explosive materials, if the person intends or knows, that such explosive materials or information will likely be used for, or in furtherance of, an activity that constitutes a Federal criminal offense or a criminal purpose affecting interstate commerce.

Id. at S7875. In conference committee, this prohibition ["the Feinstein Amendment"] was removed from the bill and was replaced with section 709 of the AEDPA -- the requirement for the Attorney General's study and report, quoted above. 142 Cong. Rec. H3336 (daily ed. Apr. 15, 1996). Senator Biden then moved to recommit the conference report to the conference committee with instructions to the Senate managers to insist on insertion of the Feinstein Amendment. 142 Cong. Rec. S3448 (daily ed. Apr. 17, 1996). Senator Hatch moved to table Senator Biden's motion, and Senator Hatch's motion was agreed to by a vote of 51 to 48. Id. at S3450.

Two months later, Senator Feinstein revived her proposal, and the Senate unanimously agreed to include it as an amendment to a bill that later became the National Defense Authorization Act for Fiscal Year 1997. 142 Cong. Rec. S7271-74 (daily ed. June 28, 1996). Once again, however, the Feinstein Amendment was removed in conference. 142 Cong. Rec. H9303 (daily ed. July 30, 1996).

I.

THE PUBLIC AVAILABILITY OF INFORMATION ON THE MANUFACTURE OF BOMBS, DESTRUCTIVE DEVICES, AND WEAPONS OF MASS DESTRUCTION

The first question that section 709 required the Attorney General to study concerns the availability of instructional information describing the fabrication of explosives, destructive devices and other weapons of mass destruction. Our study confirms that any member of the public who desires such information can readily obtain it.

A. Books, Pamphlets and Other Printed Material. Most strikingly, a cursory search of the holdings of the Library of Congress located at least 50 publications substantially devoted to such information, all readily available to any member of the public interested in reading them and copying their contents. The titles of a number of these publications are indicative of their contents.² They include:

- Guerrilla's Arsenal: Advanced Techniques For Making Explosives and Time- delay Bombs (Paladin Press, 1994);
- The Anarchist Arsenal (Harber, 1992);
- Deadly Brew: Advanced Improvised Explosives (Paladin Press, 1987);
- The Anarchist's Handbook (J. Flores, 1995);
- Improvised Explosives: How To Make Your Own (Paladin Press, 1985); and

-- Ragnar's Guide to Home and Recreational Use of High Explosives (Paladin Press, 1988).

Other texts, intended for military training, agricultural and engineering use, contain information equally useful to individuals bent upon constructing bombs and other dangerous weapons. Publications in this category include:

-- Explosives In Roadworks: User's Guide (Assoc. of Australian State Road Authorities, 1982);

-- Explosives and Blasting Procedures Manual (U.S. Bureau of Mines, 1982);

-- Military Chemical and Biological Agents: Chemical and Toxicological Properties (Telford Press, 1987); and

-- Clearing Land Of Rocks for Agricultural and Other Purposes (Institute of Makers of Explosives, 1918).

Another collection of some 48 different "underground publications" dealing with bombmaking, contained in the library of the FBI Explosives Unit, reflects a similar diversity of such published material. All of this literature was easily obtainable from commercial sources.

The ready accessibility of such literature is further illustrated by reference to a single page in a recent 70-page catalog of Delta Press, Ltd., of El Dorado, Arizona, captioned "Homemade Explosives." Among the texts featured on that page are Improvised Shape Charges, Two Component High Explosive Mixtures, Improvised Radio Detonation Techniques, and the Anarchists Handbook Series. Another page, captioned "poisons," advertises The Poisoner's Handbook, which it touts as "a complete handbook of poisons, both natural and manmade," including poisonous gases, lethal drugs, poisonous explosive compounds and a "list of sources and some additional chemistry." A number of the titles featured in this publication are commonly featured, along with firearms publications, at local gun shows.

With respect to weapons of mass destruction, there are a number of readily available books, pamphlets, and other printed materials that purport to provide information relating to the manufacture, design and fabrication of nuclear devices. The Department is aware of many publications that claim to provide some fundamentals necessary for the understanding of nuclear weapons, e.g., physics, design, manufacture, or fabrication. They include:

-- The Curve of Binding Energy (J. McPhee, 1974);

-- U.S. Nuclear Weapons: The Secret History (C. Hansen, 1966); and

-- The Swords of Armageddon (C. Hansen, 1986).³

Stories of crimes contained in popular literature and magazines also constitute a rich source of bombmaking information. For example, the August 1993 edition of Reader's Digest contains an account of efforts by law enforcement officers to track down the killer of United States Court of Appeals Judge Robert S. Vance and attorney Robert Robinson. That article contained a detailed description of the explosive devices used by the bomber in committing the murders, including such information as the size of the pipe bombs, how the bombs were constructed, and what type of smokeless powder was used in their construction.⁴ According to the Arson and Explosives Division of the Bureau of Alcohol, Tobacco and Firearms, in a bombing case originating in Topeka, Kansas, the devices were patterned after the bomb used to

kill Judge Vance. Upon questioning, the suspect admitted to investigators that he constructed the bomb based on information contained in the Reader's Digest article.

B. The Internet. Bombmaking information is literally at the fingertips of anyone with access to a home computer equipped with a modem.⁵ To demonstrate such availability, a member of the DOJ Committee accessed a single website on the World Wide Web and obtained the titles to over 110 different bombmaking texts, including "Calcium Carbide Bomb," "Jug Bomb," "How To Make a CO2 Bomb," "Cherry Bomb," "Mail Grenade," and "Chemical Fire Bottle." The user could access and print the text of each of the listed titles.⁶

One of the texts, captioned "Nifty Things That Go Boom," appears to be a computer adaptation of The Terrorist's Handbook (purportedly edited at Michigan State University). The publication contains chapters that describe and address the procurement (legal and otherwise) of necessary explosives, chemicals and other ingredients, the preparation of chemicals, techniques for transforming such substances into bombs and explosives, and the manufacture of fuses and other ignition systems.

Another of the accessed texts purports to consist of the "Bomb Excerpts" from Anarchy Cookbook. This text explains in minute detail how to construct dozens of different types of bombs and explosive devices, including fertilizer bombs, dynamite and other explosives made with chemicals and other substances that "can be bought at Kmart, and various hardware supply shops." The text also details the ways that such devices can be employed following their fabrication. For example, discussing the use of a bomb constructed from a CO2 cartridge and black powder, it explains:

Insert a fuse. . . . Now, light it and run like hell! It does wonders for a row of mailboxes (like the ones in apartment complexes), a car (place under the gas tank), a picture window (place on window sill), a phone booth (place right under the phone), or any other devious place. This thing throws shrapnel, and can make quite a mess!

Similarly, after explaining how to build a thermite bomb, the manual explains:

Now when you see your victim's car, pour a fifty-cent sized pile onto his hood, stick the [magnesium] ribbon in it, and light it with a blow torch. Now chuckle as you watch it burn through the hood, the block, and axle, and the pavement. BE CAREFUL! The ideal mixtures can vaporize CARBON STEEL! Another idea is to use thermite to get into pay phone and cash boxes. HAVE FUN!

And, in discussing how to construct a thermite letter bomb using an insulated, padded mailing envelope, the author explains that, when the detonating "explosive is torn or even squeezed hard it will ignite the powdered magnesium . . . and then it will burn the mild thermite. If the thermite didn't blow up, it would at least burn the fuck out of your enemy (it does wonders on human flesh!)."⁷

Our review of material accessible on the Internet also reveals the frequent use of "Usenet" newsgroups to facilitate the exchange of information concerning the fabrication and use of explosives and other dangerous

weapons. For example, on August 28, 1996, one participant of a Usenet newsgroup inquired whether anyone had a recipe for C-4 and detonation techniques. The following day, someone responded to the inquiry by posting a detailed formula, explaining that "[t]he production of C-4 is probably beyond what can [be] done in the kitchen, but here is something to get you started." On August 16, 1996, another Usenet participant complained that he had "recently attempted to follow the recipe [for an explosive] posted earlier . . . and nearly blew my arms off!" This prompted the following response:

So what do you want, sympathy? Let me clue you in here. Actually building any of this stuff is illegal, immoral, anti-social, and just plain wrong. But then, so are a lot of other fun things. The point is, if you do it, and you blow yourself up, it's your own fault. So quit sniveling. [N]ext time, don't cook at home.

C. Summary. It is readily apparent from our cursory examination that anyone interested in manufacturing a bomb, dangerous weapon or weapon of mass destruction can easily obtain detailed instructions for fabricating and using such a device. Available sources include not only publications from the so-called underground press but also manuals written for legitimate purposes, such as military, agricultural, industrial and engineering purposes. Such information is also readily available to anyone with access to a home computer equipped with a modem.

II. THE EXTENT TO WHICH PUBLISHED BOMBMaking INFORMATION HAS FACILITATED THE MANUFACTURE AND USE OF EXPLOSIVES IN ACTS OF TERRORISM AND OTHER CRIMINAL ACTIVITY

Recent law enforcement experience demonstrates that persons who attempt or plan acts of terrorism often possess literature that describes the construction of explosive devices and other weapons of mass destruction (including biological weapons). Although in some cases there is no hard evidence demonstrating that such individuals actually employed such information in furtherance of their crimes, possession of such information often is strong circumstantial evidence from which such usage can be inferred.

During the execution of a search warrant at the Rex, Georgia residence of Walter Leroy Moody, Jr., the convicted bombing murderer of Judge Robert S. Vance and attorney Robert Robinson, investigators discovered a copy of the Anarchist's Cookbook.

In November 1995, Oklahoma residents Ray and Cecilia Lampley, along with one John "J.D." Baird, began construction of an ammonium nitrate bomb, utilizing a manual for the making of "Homemade C-4," a military plastic explosive. The group intended to destroy either the Jewish Anti-Defamation League building in Houston, Texas, or the Southern Poverty Law Center in Birmingham, Alabama. Following the recipe from the manual, the Lampleys "cooked" the ammonium nitrate, and obtained accelerants, such as nitromethane and powdered aluminum. Additionally, Ray Lampley learned that he needed an initial detonating charge to properly detonate the "homemade C-4," and attempted to make a triacetone triperoxide detonator utilizing instructions from Ragnar's Big Book of Explosives. When the three co-conspirators were arrested by the FBI, law enforcement agents recovered the Anarchist's Cookbook and Homemade Weapons, in addition to the "homemade C-4" text, from the Lampley residence.⁸

Following the February 26, 1993, terrorist bombing of the World Trade Center in New York City, investigators discovered bombmaking manuals in the possession of individuals connected with that crime. Although it is believed that those individuals brought those particular manuals into the United States from a foreign country, the manuals had been copied from books written and printed in the United States and available for purchase from publishers like Paladin Press. The presence of these manuals suggests that the conspirators consulted them in effecting their deadly terrorist scheme.

Between January 1994 and January 1996, a string of some 18 bank robberies occurred across the Midwest. The robberies were committed by individuals brandishing automatic weapons, wearing disguises, and using hoax-bomb devices, apparently to delay pursuit and investigation. Following the arrests of two individuals linked to the series of robberies, investigators conducted searches of safehouses and other locations used by the defendants. Execution of the search warrants resulted in the discovery of numerous weapons, explosives, grenades, and components for manufacturing improvised explosive devices. Additionally, the investigators discovered a library of literature describing neo-guerrilla techniques, including the manufacture and use of explosives.

Beginning in 1991, four members of the "Patriots Council," a Minnesota tax protest group, began to develop a castor-bean derivative known as "ricin," which is one of the most toxic known substances. The members involved learned the process of manufacturing ricin from a mail-order pamphlet. The group planned to suspend the substance in a toxic gel capable of transmission through a skin barrier, and then to place the impregnated gel on doorknobs, handles, and steering wheels. They were considering whether to target IRS agents, U.S. Marshals, or local sheriffs for ricin attacks when the FBI arrested them.²

In 1993, Thomas Lavy attempted to cross the Canadian border carrying 130 grams of ricin -- an amount that, if administered in individual doses, would be sufficient to kill over 32,000 people -- as well as four guns and \$89,000 in cash. Canadian officials returned Lavy to the United States because of the amount of cash he was carrying. A search of Lavy's cabin by law enforcement officers revealed that he possessed mail-order books, such as The Poisoner's Handbook, Silent Death, and Get Even: The Complete Book of Dirty Tricks, which, among other things, describe how to make and use ricin. Lavy committed suicide before he could be tried.

To the Department's knowledge, no devices producing a nuclear yield have been constructed based on published bombmaking information. However, the Department is aware of approximately 117 threats since 1970 involving detonations of nuclear devices. Approximately half of these nuclear extortion threats have been accompanied by sketches, information, or descriptive phrases gleaned from information in the public domain, including technical reference materials and fictional nuclear "thrillers."

In addition to the incidents recounted above, reported federal cases involving murder, bombing, arson, and related crimes, reflect the use of bombmaking manuals by defendants and the frequent seizure of such texts during the criminal investigation of such activities. See, e.g., United States v. Prevatte, 66 F.3d 840, 841 (7th Cir. 1995) (bombmaker read Anarchist's Cookbook); United States v. Johnson, 9 F.3d 506, 510 (6th Cir. 1993) (search of bombmaker's residence revealed presence of books on explosive devices), cert. denied, 512 U.S. 1212 (1994); United States v. Talbott, 902 F.2d 1129, 1131 (4th Cir. 1990) (execution of search warrant at residence of bombmaker revealed presence of books on bombmaking); United States v. Michael, 894 F.2d 1457, 1459 (5th Cir. 1990) (bombmaker bought books at gun shows to determine how to make bombs, booby traps and silencers); United States v. Levasseur, 816 F.2d 37, 41 (2d Cir. 1987) (execution of search warrant at bomber's residence revealed presence of bombmaking instructions); United States v. Arocena, 778 F.2d

943, 947 (2d Cir. 1985) (members of "Omega 7" group, who conducted terrorist bombings in New York metropolitan area, possessed bombmaking manuals), cert. denied, 475 U.S. 1053 (1986); United States v. Williams, 775 F.2d 1295, 1298 (5th Cir. 1985) (bomb murderer used Marine Corps training manual to construct "mouse trap" bomb), cert. denied, 475 U.S. 1089 (1986); United States v. Bergner, 800 F. Supp. 659, 663 (N.D. Ind. 1992) (bomber consulted Anarchist's Cookbook and other bombmaking texts available at police academy library).

Finally, information furnished by the Bureau of Alcohol, Tobacco and Firearms reveals that such literature is frequently used by individuals bent upon making bombs for criminal purposes. ATF statistics reflect that, between 1985 and June 1996, the investigations of at least 30 bombings and four attempted bombings resulted in the recovery of bombmaking literature that the suspects had obtained from the Internet. Most recently, on August 6, 1996, ATF investigators participated in the investigation of two North Attleboro, Massachusetts, juveniles, aged 11 and 14, who were injured while attempting to make an improvised explosive device. The youths had retrieved from the Internet information on how to make napalm, and were badly burned when a mixture being heated on a kitchen stove ignited.¹⁰

In sum, it is fair to conclude from scenarios such as those we have described that the availability of bombmaking literature may play a significant role in aiding those intent on using explosives and other weapons of mass destruction for criminal purposes, including acts of terrorism. Moreover, the availability of this information might contribute to youthful experimentation with explosive devices, which could result in serious injury.

III. THE LIKELIHOOD THAT PUBLISHED BOMBMAKING INFORMATION WILL CONTINUE TO BE USED TO FACILITATE ACTS OF TERRORISM AND OTHER CRIMINAL ACTIVITY

It is, of course, impossible to prognosticate with any measure of certainty the extent to which persons wishing to engage in acts of terrorism and other criminal activity will rely upon printed and computer-based information instructing them how to manufacture bombs, other dangerous weapons, and weapons of mass destruction. A statistical survey conducted by the FBI concerning bombing incidents occurring in the United States shows that between 1984 and 1994, the frequency of such incidents has increased almost four-fold. The study, however, did not attempt to correlate the trend with the increased availability of bombmaking information. Therefore, we have no empirical data on what percentage, if any, of the recent increase in the number of bombings is attributable to the increased availability of bombmaking information. However, based upon the recent experiences recounted above, both the FBI and ATF expect that because the availability of such information is becoming increasingly widespread, such bombmaking instructions will continue to play a significant role in aiding those intent upon committing future acts of terrorism and violence.

IV. APPLICABILITY OF CURRENT FEDERAL LAW TO THE PUBLICATION AND DISSEMINATION OF BOMBMAKING INFORMATION

Presently there are four basic ways in which dissemination of bombmaking information could be punished under federal criminal law, depending on the circumstances of the case.¹¹ The first three bases for culpability -- federal statutes prohibiting (i) conspiracy, (ii) solicitation, and (iii) aiding and abetting -- do not single out information concerning bombmaking for special treatment. The fourth basis for culpability -- 18 U.S.C. § 231 -- is directed specifically at the "teaching or demonstrating" of techniques related to the use or manufacture of firearms and explosives.¹²

A. Conspiracy. A conspiracy to use an explosive to commit "any felony which may be prosecuted in a court of the United States," 18 U.S.C. § 844(h), is explicitly proscribed under 18 U.S.C. § 844(m); and a conspiracy to commit any offense defined in Chapter 40 of Title 18, U.S. Code -- entitled "Importation, Manufacture, Distribution, and Storage of Explosive Materials" -- is prohibited by 18 U.S.C. § 844(n). In addition, the general federal criminal conspiracy statute, 18 U.S.C. § 371 -- which prohibits conspiring "to commit any offense against the United States" -- makes it unlawful to conspire to commit other federal crimes involving explosives. A person may not, as part of a conspiracy to commit an independently defined criminal offense, transmit information to a coconspirator concerning how to make or use explosive devices.¹³ Indeed, such transmission of information could be an overt act in support of a conspiracy.¹⁴

In order to prove that a person disseminating bombmaking information did so as part of a conspiracy to commit a substantive offense, the government need not prove that the substantive offense occurred; however, the government must show, at the very least, that the disseminator (i) knew of the intended unlawful use of the information and (ii) agreed with other conspirators that an offense would be committed.¹⁵ And, as a general matter, the requisite agreement cannot be proved simply by demonstrating that a person has provided a product to another person knowing that the product would be used in the commission of a crime, where the provider of the product is indifferent to its subsequent use.¹⁶ "[A] conspiracy requires agreement, and there is a difference between knowing that something will occur [by virtue of one's sale of a product] -- even as an absolute certainty -- and agreeing to bring that same 'something' about." United States v. Lechuga, 994 F.2d 346, 362 (7th Cir.) (Cudahy, J., concurring in pertinent part), cert. denied, 510 U.S. 982 (1993). It follows that "an isolated sale is not the same thing as enlisting in the venture." United States v. Blankenship, 970 F.2d 283, 287 (7th Cir. 1992).¹⁷

B. Solicitation. The federal criminal solicitation statute, 18 U.S.C. § 373, provides in pertinent part:

Whoever, with intent that another person engage in conduct constituting a felony that has as an element the use,
 attempted use, or threatened use of physical force against property or against the person of another in violation
 of the laws of the United States, and under circumstances strongly corroborative of that intent, solicits, commands,
 induces, or otherwise endeavors to persuade such other person to engage in such conduct, shall be imprisoned not
 more than one-half the maximum term of imprisonment or (notwithstanding section 3571) fined not more than one-half
 of the maximum fine prescribed for the punishment of the crime solicited, or both; or if the crime solicited is punishable
 by life imprisonment or death, shall be imprisoned for not more than twenty years.

Id. § 373(a). Solicitation proscribed by this statute often will take the form of speech, including written speech.¹⁸ Indeed, Congress intended that the statutory phrase "otherwise endeavors to persuade" be construed broadly to cover any situation "where a person seriously seeks to persuade another person to engage in criminal conduct." *United States v. Buckalew*, 859 F.2d 1052, 1054 (1st Cir. 1988) (Breyer, J.) (quoting S. Rep. No. 307, 97th Cong., 1st Sess. 183-84 (1982)) (emphasis added). In the prototypical solicitation case, the "persuasion" is accompanied by some form of inducement, such as a money payment, or a threat. Such a case raises no First Amendment issues, for reasons we explain *infra* at 35-38.¹⁹ However, insofar as Congress also intended § 373 to cover cases of "persuasion" taking the form of mere advocacy or urging of unlawful action -- without any threat or inducement -- many such cases could be subject to significant First Amendment constraints under the *Brandenburg* doctrine. *See infra* at 29-30 (discussing *Brandenburg v. Ohio*, 395 U.S. 444 (1969)).²⁰ Therefore, for purposes of this discussion, we will assume that § 373 would be used principally in the case of "persuasion" accompanied by an inducement (e.g., murder for hire²¹) or an explicit or implicit threat or "command" (e.g., an organized crime boss "asking" an associate to commit a crime).

In such cases, the solicitation itself would not likely be in the form of a transmission of bombmaking information. However, as part of a solicitation scheme, it is conceivable that the solicitor would transmit such information so as to facilitate the crime being solicited. Indeed, such facilitation could provide circumstances that "strongly corroborate" a solicitor's improper intent, thereby satisfying § 373's scienter requirement: Congress indicated that it would be "highly probative" of improper intent if the solicitor "acquired . . . information suited for use by the person solicited in the commission of the offense, or made other apparent preparations for the commission of the offense by the person solicited." S. Rep. No. 307, 97th Cong., 1st Sess. 183 (1982).

Although § 373 does not require either actual agreement (like conspiracy), nor that the crime be committed (like aiding and abetting), it nonetheless could provide a means of addressing dissemination of bombmaking information in only a limited set of cases. For one thing, the statute requires more than mere dissemination of information: there must be some solicitation, command, inducement or other endeavor to persuade. (And the First Amendment might exclude cases of "persuasion" absent any threat, command or inducement.) More importantly, the government must prove "circumstances strongly corroborative" of the solicitor's intent that another person engage in conduct constituting a felony.

C. Aiding and Abetting. Two different "aiding and abetting" statutes might have some application in cases where bombmaking information is disseminated: (i) the general federal aiding and abetting statute, 18 U.S.C. § 2, and (ii) section 323 of the AEDPA, which concerns provision of material support or resources for use in certain crimes of terrorism.

1. 18 U.S.C. § 2. In 1909 Congress enacted what is now 18 U.S.C. § 2, a general aiding and abetting statute applicable to all federal criminal offenses. That statute in essence provides that "those who provide knowing aid to persons committing federal crimes, with the intent to facilitate the crime, are themselves committing the crime." *Central Bank of Denver, N.A. v. First Interstate Bank of Denver, N.A.*, 511 U.S. 164, 181 (1994) (citing *Nye & Nissen v. United States*, 336 U.S. 613, 619 (1949)).²² Not infrequently, aiding and abetting can take the form of speech, including providing instructions on how to commit a crime to a particular person or to a discrete audience.²³ Section 2 nonetheless is somewhat ineffectual as a tool to address dissemination of information on how to manufacture explosives, for three reasons.

First, there is some question whether aiding and abetting culpability ever can rest solely on the basis of general publication of instructions on how to commit a crime, or undifferentiated sale to the public of a product that some purchaser is likely to use for unlawful ends, or whether, at a minimum, the person supplying the aid must know that a particular recipient thereof will use it in commission of a crime.²⁴

Second, even assuming that aiding and abetting could under some circumstances be established by virtue of a publisher's knowledge that unknown recipients of generally published information would use it to commit crimes, § 2 requires that the accomplice have engaged in intentional wrongdoing, rather than mere recklessness. Central Bank of Denver, 511 U.S. at 190. That is to say, the aider must not only know that her assistance will be in the service of a crime; she also must share in the criminal intent. The defendant must "participate in [the venture] as in something that he wishes to bring about, that he seek by his action to make it succeed." Nye & Nissen, 336 U.S. at 619 (quoting United States v. Peoni, 100 F.2d 401, 402 (2d Cir. 1938)).²⁵ As Judge Hand explained in the seminal Peoni case, the intent standard for criminal aiding and abetting is not the same as the "natural consequences of one's act" test that is the touchstone for "intent" in the civil tort context; criminal intent to aid the crime has "nothing whatever to do with the probability that the forbidden result [will] follow upon the accessory's conduct." Peoni, 100 F.2d at 402. Rather, the aider must have a "purposive attitude" toward the commission of the offense. Id.²⁶

Finally, under the plain terms of § 2, the underlying offense must in fact be committed (though the government need not prove by whom it was committed); section 2 merely makes aiders and abettors culpable for their principals' commission of an offense.²⁷ There is no federal statute generally proscribing an attempt to aid and abet a federal offense (though the Model Penal Code recommended that such a prohibition be codified).²⁸ Therefore, if a crime has not been committed, the general federal aiding and abetting statute cannot be invoked.

2. AEDPA Section 323. Section 323 of the AEDPA, 110 Stat. at 1255 (to be codified as amended section 2339A(a) of Title 18) makes it unlawful to provide "material support or resources" to another person, "knowing or intending that they are to be used in preparation for, or in carrying out," various federal offenses relating to terrorism, or in preparation for, or in carrying out, the concealment from the commission of any such violation. Id. (to be codified at 18 U.S.C. § 2339A(a)).²⁹ Notably, the statute defines the term "material support or resources" to include, inter alia, "training, . . . and other physical assets." Id. (to be codified at 18 U.S.C. § 2339A(b)).³⁰

Section 323 essentially is a prohibition on certain forms of knowing or intentional facilitation of particular terrorist crimes. In two respects, it is broader in scope than the general aiding and abetting statute. First, the facilitator can be culpable even if the underlying offense is not in fact committed. Second, the scienter provision is a bit broader than the "intent" requirement in 18 U.S.C. § 2. Under AEDPA section 323, specific intent to facilitate the underlying offense is not necessary:³¹ the person providing the support or resources can be culpable so long as he "know[s]" that the resources provided "are to be used" to prepare for or commit a specified offense. In effect, however, this "knowledge" provision will rarely be of use to a prosecutor, because where -- as in section 323 -- the element of "knowledge" refers to a possible future result of a defendant's conduct, typically the government must prove that the defendant was "aware that that result is practically certain to follow from his conduct." United States v. Bailey, 444 U.S. 394, 404 (1980) (emphasis added) (quoting United States v. United States Gypsum Co., 438 U.S. 422, 445 (1978) (internal citation omitted)).³²

Furthermore, whatever the scope of the "knowledge" provision, the use of section 323 to address distribution of bombmaking information might nonetheless be limited, for two other reasons. First, section 323 covers facilitation of only certain enumerated crimes. Seesupra note 29. Second, it is not clear whether courts would find that information on how to manufacture or use explosives is "material support or resources." In the case of an actual physical demonstration of the techniques in question, or a one-to-one sale of printed information to someone who purports to be planning a crime, transfer of such information might constitute "training." Otherwise, it is open to question whether a manual on explosives would constitute a "physical asset[]" under § 2339A. ³³

D. 18 U.S.C. § 231(a)(1). For the most part, the federal statutes discussed in the previous sections are not directed at dissemination of information, as such. Instead, they are general prohibitions on conduct that can, in particular cases, be violated by providing information to another person.

By contrast, 18 U.S.C. § 231(a)(1) -- like the proposed Feinstein Amendment -- arguably could be characterized as a prohibition on certain forms of speech. Section 231(a)(1) provides that:

Whoever teaches or demonstrates to any other person the use, application, or making of any firearm or explosive or incendiary device, or technique capable of causing injury or death to persons, knowing or having reason to know or intending that the same will be unlawfully employed for use in, or in furtherance of, a civil disorder which may in any way or degree obstruct, delay, or adversely affect commerce or the movement of any article or commodity in commerce or the conduct or performance of any federally protected function . . . [s]hall be fined under this title or imprisoned not more than five years, or both.

"Civil disorder," in turn, is defined as "any public disturbance involving acts of violence by assemblages of three or more persons, which causes an immediate danger of or results in damage or injury to the property or person of any other individual." 18 U.S.C. § 232(1).

This prohibition applies, not to all forms of speech that could cause a civil disorder, but solely to a discrete type of conduct involving expression -- namely, the "teach[ing]" or "demonstrat[ion]" of the use, application, or making of any firearm or explosive or incendiary device, or technique capable of causing injury or death to persons. ³⁴

It appears that this statute has been used sparingly; there are only two reported decisions involving it. ³⁵ In those two cases, the courts of appeals narrowly construed the scienter provisions of § 231(a)(1) so as to avoid serious constitutional questions. National Mobilization Comm. to End the War in Viet Nam v. Foran, 411 F.2d 934 (7th Cir. 1969); United States v. Featherston, 461 F.2d 1119 (5th Cir.), cert. denied, 409 U.S. 991 (1972). In both cases, the persons charged under § 231(a)(1) were alleged to have instructed discrete groups of students on techniques of violence, with the intent that such techniques would be used in furtherance of civil disorders. The defendants nonetheless complained that the statute was impermissibly vague or overbroad, because its plain terms are not limited to cases of bad intent. Read literally, § 231(a)(1) also could be construed to prohibit well-intentioned persons from teaching techniques of self-defense and sporting activities where such persons have a "reason to know" that some pupils might put the skills they acquire to

unlawful use. The defendants in Foran and Featherston argued that this apparent reach of § 231(a)(1) rendered the statute facially invalid under the First Amendment.

In order to avoid the substantial constitutional questions raised by the "reason to know" language, both courts of appeals construed the scienter element of § 231(a)(1) narrowly. The Seventh Circuit, somewhat cryptically, concluded that "[t]he requirement of intent of course `narrows the scope of the enactment by exempting innocent or inadvertent conduct from its proscription." Foran, 411 F.2d at 937 (citation omitted). The Fifth Circuit, relying upon the Supreme Court's narrowing construction of similar language in an espionage statute, held that proof of "'bad faith'" is required under § 231(a)(1). Featherston, 461 F.2d at 1121 (quoting Gorin v. United States, 312 U.S. 19, 27-28 (1941)). The court concluded that "the statute does not cover mere inadvertent conduct. It requires those prosecuted to have acted with intent or knowledge that the information disseminated would be used in furtherance of a civil disorder." Id. at 1122 (emphasis added).

The potential use of § 231(a)(1) to reach cases involving dissemination of bombmaking information is limited in three ways. First, as construed in Featherston and Foran, § 231(a)(1) can apply only where the person doing the teaching or demonstrating either (i) intends that the information will be used in furtherance of a civil disorder or (ii) "knows" that the information will be so used. As explained supra at 21, as a practical matter the "or knows" prong will rarely be useful: since the knowledge in question is of a possible future result of a defendant's conduct, the government must prove that the defendant was "aware `that that result is practically certain to follow from his conduct.'" Bailey, 444 U.S. at 404 (citations omitted) (emphasis added).³⁶ Accordingly, the vast majority of cases in which § 231(a)(1) could successfully be invoked will involve defendants who intend that their teaching be used to facilitate or assist in a civil disorder.

Second, it is questionable whether the operative verbs -- "teaches or demonstrates" -- could be read to cover an arms-length sale of a manual to an anonymous or unknown customer. Finally, the intended or known use of the information conveyed must be "in, or in furtherance of, a civil disorder which may in any way or degree obstruct, delay, or adversely affect commerce or the movement of any article or commodity in commerce or the conduct or performance of any federally protected function." And a "civil disorder" requires a public disturbance involving violence by assemblages of three or more persons. Section 231(a)(1) would not, therefore, apply to uses of the information by merely one or two felons.

V. THE NEED FOR ADDITIONAL LAWS RELATING TO THE DISSEMINATION OF BOMBMAKING INFORMATION

During the Senate debate on the Feinstein Amendment, Senators Feinstein and Biden identified two sets of circumstances in which the dissemination of bombmaking information ideally should be prohibited:

- (i) where the person disseminating the information intends that it be used for unlawful ends;³⁷ and

(ii) where the person disseminating the information has good reason to know that a particular potential recipient thereof plans to use that information to engage in unlawful activities.³⁸

On the other hand, Senator Feinstein made it plain that she did not wish to prohibit the "legitimate" publication of information about explosives contained in, for instance, the Encyclopedia Britannica (despite the fact that such information certainly could be used by persons who wished to commit violent crimes);³⁹ and Senator Hatch indicated that any prohibition that is enacted should be drafted carefully, so as not to subject to criminal sanctions, for example, legitimate explosives manufacturers who teach customers and other persons how to manufacture, and make legitimate use of, explosives.⁴⁰

The Department of Justice agrees that it would be salutary if the federal criminal law prohibited dissemination of bombmaking information in the two circumstances described above, while still permitting the "legitimate" publication of information about explosives in the manner described by Senators Feinstein and Hatch. As the discussion in Part IV demonstrates, however, the present federal criminal code is less than completely effective in accomplishing these objectives:

1. Federal law would in certain cases prohibit or punish the dissemination of bombmaking information where the person disseminating the information intends that it be used for unlawful ends. For example:

-- If the disseminator enters into an agreement with another person to commit a federal crime, dissemination of bombmaking information as a means of furthering that crime would be an overt act in furtherance of a conspiracy. Similarly, if the disseminator solicits another person to commit a federal crime of violence -- for example, by offering a reward for its commission -- conveyance of the bombmaking information would be evidence "strongly corroborating" an improper intent, thereby satisfying the scienter requirement of 18 U.S.C. § 373.

-- If the disseminator provides the information to a particular person with the specific purpose of assisting the recipient in the commission of a federal crime, and if the recipient thereafter does commit such an offense, the disseminator would be culpable for aiding and abetting that offense. And, even if the offense is not in fact committed, the disseminator might still be culpable for a violation of AEDPA section 323, provided (i) that the offense that he intended to advance was one of those enumerated in the statute; and (ii) a court finds that bombmaking information can be considered "material support or resources."

-- If the disseminator provides the information to a person or persons in order to prepare for or further a "civil disorder," he will have violated 18 U.S.C. § 231(a)(1), assuming that provision of such information constitutes the "teach[ing] or demonstrat[ion]" of the making of explosives or incendiary devices.

However, except where the particular requirements of AEDPA section 323 or 18 U.S.C. § 231(a)(1) are met, federal law presently does not provide a ground for prosecution where a disseminator of bombmaking information does not conspire with or solicit another to commit a federal crime, but nevertheless intends to aid the recipients of the information in commission of such criminal conduct, and where no federal crime is in fact committed. Further, federal law does not presently reach the person who disseminates bombmaking information intending that it be used to aid the commission of a state or local criminal offense, notwithstanding the utilization of interstate or foreign commerce to achieve such dissemination and notwithstanding the actual or potential impact of the underlying violation on such commerce.

2. If a disseminator of bombmaking information does not have the specific purpose of facilitating a crime, but nonetheless is aware that (i) an enumerated terrorist crime or (ii) a "civil disorder" were practically certain to follow from dissemination of the information to a particular person or persons, then the disseminator might be culpable under AEDPA section 323, or 18 U.S.C. § 231(a)(1), respectively. However, absent such a high degree of "knowledge" of the facilitation of future crimes, current federal law generally would not prohibit or punish the dissemination of bombmaking information in the case where the disseminator does not have the specific purpose of facilitating a crime but nevertheless knows that a particular recipient thereof intends to use it for unlawful ends.

In sum, current federal law does not specifically address certain classes of cases that Senators Feinstein and Biden identified. Accordingly, the Department of Justice agrees with those Senators that it would be appropriate and beneficial to adopt further legislation to address this problem directly, in a manner that does not impermissibly restrict the wholly legitimate publication and teaching of such information, or otherwise violate the First Amendment.

VI. CONSTITUTIONALITY OF RESTRICTING OR PENALIZING THE PUBLICATION OR DISSEMINATION OF BOMBMAKING INFORMATION

Before identifying what further steps Congress can take to address this problem, it is necessary to discuss whether and to what extent the First Amendment limits the government's power to impose criminal culpability on persons publishing or disseminating bombmaking information. In this regard, it should be noted that in Rice v. Paladin Enterprises, Inc., 940 F. Supp. 836 (D. Md. 1996), appeal docketed, No. 96-2412 (4th Cir.), a district court recently held that the First Amendment substantially protects the right of persons to publish such information, regardless of the publishers' intent.

The defendant in that case, publisher Paladin Enterprises, Inc., has (for many years) offered for public sale (principally through a mail-order catalogue) a book entitled Hit Man, which describes in great detail specific methods and techniques of, and strategies for, murder for hire. James Perry ordered and received Hit Man from Paladin. Thereafter, Perry followed a number of instructions in Hit Man in planning, executing, and attempting to hide the evidence of, his contract killing of three people in Montgomery County, Maryland. Perry was convicted of murder, after which the survivors of the victims sued Paladin in federal court for wrongful death, alleging that Paladin had aided and abetted the murders by selling Hit Man to Perry. Paladin moved for summary judgment on the ground that the First Amendment barred recovery. For the purposes of the motion, the parties stipulated the following:

1. Paladin had no contact with Perry (or the person who hired him to commit the murders) other than to

sell him Hit Man

and another book. Paladin had no "specific knowledge" that Perry planned to commit a crime, or that he had been

retained to kill anyone. 940 F. Supp. at 839.

2. In planning, committing, and concealing his crimes, Perry followed certain descriptions and instructions in Hit Man,

including: (a) Hit Man's recommendation that a "beginner" hit man use an AR-7 rifle; (b) Hit Man's instructions on how

to disassemble the AR-7; (c) Hit Man's detailed instructions on how to drill out the serial number on the rifle; (d) Hit

Man's detailed instructions on how to create a silencer to use on an AR-7; (e) Hit Man's detailed instructions on how to

murder victims from close range; and (f) Hit Man's detailed instructions on how to file the AR-7 so that it would not be

traceable. Id. at 839-40.⁴¹

3. Paladin engaged in a marketing strategy intended to maximize sales to the public, including sales to the following targeted

audiences: authors who desire information for the purpose of writing books about crime and criminals; law enforcement

officers and agencies who desire information concerning the means and methods of committing crimes; persons who

enjoy reading accounts of crimes and the means of committing them for purposes of entertainment; persons who

fantasize about committing crimes but do not thereafter commit them; criminologists and others who study criminal

methods and mentality; and "criminals and would-be criminals who desire information and instructions on how to commit

crimes." In particular, the parties stipulated that "[i]n publishing, marketing, advertising and distributing Hit Man . . . ,

Paladin intended and had knowledge that their publications would be used, upon receipt, by criminals and would-be

criminals to plan and execute the crime of murder for hire, in the manner set forth in the publications." Id. at 840.⁴²

The district court granted Paladin summary judgment. The court seemed to rely upon two distinct rationales for its decision: First, the court concluded that the State of Maryland has not "extend[ed] the tort of aiding and abetting to the circumstances of this case," and that "[a] federal court sitting in diversity cannot create new causes of action." Id. at 842. Accordingly, the court seemed to conclude that plaintiffs had failed to state a claim under Maryland tort law. Id. Second, the court held that, even if an aiding and abetting tort theory were cognizable, Paladin's publication and dissemination of the book was entitled to constitutional protection, and "the First Amendment acts as a bar to liability in the instant case," id. at 843, despite defendants' stipulation that they "intended and had knowledge that their publications would be used, upon receipt, by criminals and would-be criminals to plan and execute the crime of murder for hire, in the manner set forth in the publications." See also id. at 843-49 (First Amendment analysis).

This recent decision suggests that it is necessary to consider carefully the First Amendment questions that a statute like the Feinstein Amendment would raise.⁴³

A. First Amendment Principles

Other than the cursory analysis in the Featherston and Foran cases, discussed *supra* at 22-23, and the district court's recent decision in Rice v. Paladin, discussed *supra* at 27-28, there is little in the way of judicial analysis directly addressing the First Amendment questions that a statute like the Feinstein Amendment would raise.⁴⁴ However, the courts have substantially addressed the scope of the Free Speech Clause in three related factual contexts that serve to put the constitutional question in perspective: (i) where the government seeks to restrict the advocacy of unlawful action; (ii) where the government (or a private party using tort law) seeks to restrict or punish the general disclosure or publication of lawfully obtained information; and (iii) where the government punishes conveyance of information as part of a "speech act," such as speech that aids and abets another person's commission of a crime.

1. Advocacy of Unlawful Action. In the landmark case of Brandenburg v. Ohio, 395 U.S. 444 (1969) (*per curiam*), the Supreme Court held that "the constitutional guarantees of free speech and free press do not permit a State to forbid or proscribe advocacy of the use of force or of law violation except where such advocacy is directed to inciting or producing imminent lawless actions and is likely to incite or produce that action." *Id.* at 447 (footnote omitted). This test, in other words, requires both an intent and a likelihood that the expression in question -- "advocacy of the use of force or of law violation " -- will incite or produce imminent unlawful action.

A few years later, the Court made clear how demanding the Brandenburg test is. In Hess v. Indiana, 414 U.S. 105 (1973) (*per curiam*), the defendant was arrested for loudly stating, at an anti-war rally, "We'll take the fucking street later." The Court held that Brandenburg prohibited the State from punishing this alleged advocacy of illegality, principally because the defendant's statement "amounted to nothing more than advocacy of illegal action at some indefinite future time." *Id.* at 108. Furthermore, the Court reasoned that "[s]ince the uncontroverted evidence showed that Hess' statement was not directed to any person or group of persons, it cannot be said that he was advocating, in the normal sense, any action." *Id.* at 108-09.

In light of these precedents,⁴⁵ it is doubtful that general publication of written materials advocating illegality can ever be proscribed under the Brandenburg test.⁴⁶ Many of the bombmaking manuals discussed by Congress and identified in this Report could plausibly be said to advocate -- either explicitly or implicitly -- the illegal use of explosives and other weapons. Insofar as publication of such manuals were criminalized on account of those manuals' advocacy of unlawful conduct, such a prohibition almost certainly could not pass constitutional muster.⁴⁷

2. Disclosure or Publication of Lawfully Obtained Information. The Brandenburg test, by its terms, applies to advocacy of unlawful conduct. But the government's principal concern with respect to bombmaking manuals is not their advocacy, but the instructional information they contain. That information is (at least for the most part) a matter of public record. As demonstrated elsewhere in this Report, anyone interested in manufacturing a bomb, dangerous weapon or weapon of mass destruction can easily obtain detailed instructions for manufacturing and using such a device, both from legitimate publications and from so-called "underground" publications. And, presumably, most if not all of the writers and publishers of such

publications do not obtain the information unlawfully, or from classified sources. The First Amendment imposes significant constraints on the ability of the government to restrict publication of such information.

Although the Supreme Court has been careful never to hold categorically that publication of lawfully obtained truthful information "is automatically constitutionally protected," The Florida Star v. B.J.F., 491 U.S. 524, 541 (1989), nonetheless the Court has, on several occasions, held that "the government may not generally restrict individuals from disclosing information that lawfully comes into their hands in the absence of a `state interest of the highest order.'" United States v. Aguilar, 115 S. Ct. 2357, 2365 (1995) (quoting Smith v. Daily Mail Pub. Co., 443 U.S. 97, 103 (1979)). See also Butterworth v. Smith, 494 U.S. 624, 632 (1990). And even if the state has such an interest, "punishment may lawfully be imposed, if at all, only when narrowly tailored to a state interest of the highest order." Florida Star, 491 U.S. at 541.⁴⁸

We can assume that there is a "state interest of the highest order" in keeping information on how to make explosives out of the hands of persons who want -- or who would be likely -- to use that information in furtherance of violent crime.⁴⁹ What is more, it is "foreseeable," in the tort-law sense, that some readers will use such information for unlawful ends if the information is made publicly available. As explained in Part II of this Report, strong circumstantial evidence demonstrates that persons bent upon committing acts of terrorism often rely upon literature for guidance in the construction of explosive devices and other weapons of mass destruction. Therefore, chances are that even "legitimate" publication of bombmaking information -- such as that found in government-issued manuals and in encyclopedias -- will facilitate some degree of unlawful conduct.

Nevertheless, even where it is foreseeable that widely disseminated information will be used unlawfully, or in a negligent and dangerous manner, courts uniformly have found that the Constitution prohibits imposing culpability or civil liability for distributing or publishing that information. For example, a number of courts have held that the First Amendment prohibits imposing tort liability on publishers, producers and broadcasters for the foreseeable consequences of their speech where viewers or readers mimicked unlawful or dangerous conduct that had been depicted or described, even if the standards for tortious negligence or recklessness were otherwise satisfied.⁵⁰ Similarly, a number of courts have held that the First Amendment bars recovery for allegedly foreseeable injuries suffered by persons who were following "how-to" instructions.⁵¹ In a third, related category of cases, courts have held that the Constitution does not permit imposition of criminal penalties or civil liability for written or visual depictions

-- including depictions of "factual" events -- that are likely to alter (or that have in fact changed) persons' attitudes such that those persons are more likely to engage in criminal, dangerous or otherwise undesirable behavior.⁵²

Florida Star explicitly leaves open the possibility that, in rare circumstances, the First Amendment might not bar sanctions for the publication of true, lawfully obtained information.⁵³ Nevertheless, such an exception almost certainly would not be recognized where, as here, the information is already in the public domain. The Court's stringent First Amendment test for restrictions on publication of lawfully obtained information, in other words, almost certainly would not permit the government to proscribe the publication or widespread dissemination of bombmaking manuals. Where similar or equivalent information is widely available elsewhere, the Court has been unwilling to find that a restriction on publication of that information is "narrowly tailored" to address a state interest: no "meaningful public interest" can be served by further restriction under such circumstances. Florida Star, 491 U.S. at 535. "[O]nce the truthful information [is]

"publicly revealed" or "in the public domain," its dissemination cannot constitutionally be restrained. Id. (quoting Smith, 443 U.S. at 103 (internal citation omitted)). See also id. at 539 (one critical problem with the rape-shield statute at issue in Florida Star was that it punished publication of rape victims' identities "regardless of whether the identity of the victim is already known throughout the community").⁵⁴ Congress presumably would not be willing to ban the publication and teaching of all information concerning the manufacture of explosives -- including, for example, information exchanged among professional explosives manufacturers, or contained in the Encyclopedia Britannica and in government manuals. See supra at 24. As long as this is the case, it is hard to imagine that the First Amendment would permit culpability or liability for publication of other bombmaking manuals that have a propensity to be misused by some unknown, unidentified segment of the readership, since sources of the same information inevitably will remain in the public domain, readily available to persons who wish to manufacture and use explosives.

3. "Speech Acts," such as Aiding and Abetting. On the other hand, the constitutional analysis is radically different where the publication or expression of information is "brigaded with action,"⁵⁵ in the form of what are commonly called "speech acts." If the speech in question is an integral part of a transaction involving conduct the government otherwise is empowered to prohibit, such "speech acts" typically may be proscribed without much, if any, concern about the First Amendment, since it is merely incidental that such "conduct" takes the form of speech. "[I]t has never been deemed an abridgement of freedom of speech or press to make a course of conduct illegal merely because the conduct was in part initiated, evidenced, or carried out by means of language, either spoken, written, or printed." Ohralik v. Ohio State Bar Ass'n, 436 U.S. 447, 456 (1978) (quoting Giboney v. Empire Storage & Ice Co., 336 U.S. 490, 502 (1949)). For example, as the Court in Ohralik explained, there are "numerous examples" of communications -- including communications that convey information -- that are subjected to economic or commercial regulation without implicating the First Amendment, such as: exchange of securities information; corporate proxy statements; exchange of information among competitors; and employers' threats of retaliation for employees' labor activities. Id. (citations omitted).⁵⁶

Similarly, many inchoate crimes often or always are effected through speech "acts." Such crimes include conspiracy, facilitation, solicitation, bribery, coercion, blackmail, and aiding and abetting.⁵⁷ Punishing speech -- including the dissemination of information -- when it takes the form of such criminal conduct typically does not even raise a First Amendment question. As Justice (then-Judge) Kennedy explained, "where speech becomes an integral part of the crime, a First Amendment defense is foreclosed even if the prosecution rests on words alone." United States v. Freeman, 761 F.2d 549, 552 (9th Cir. 1985), cert. denied, 476 U.S. 1120 (1986).⁵⁸

In particular, "[t]hat 'aiding and abetting' of an illegal act may be carried out through speech is no bar to its illegality." National Org. for Women v. Operation Rescue, 37 F.3d 646, 656 (D.C. Cir. 1994).⁵⁹ What is more, aiding and abetting a crime often consists of providing factual information to another person. The role of a lookout at a burglary is to inform confederates that someone is coming. An accomplice of a bank robbery might abet the operation by telling the principal the combination of a safe, or how to evade detection. The First Amendment is simply inapposite in such cases.⁶⁰ Nor is the situation necessarily different where the information conveyed is already publicly available. For example, there may be many lawful -- and constitutionally protected -- circumstances in which a person (say, a professor of architecture) may provide the blueprint of a bank to other persons (say, architecture students); but if such blueprints are transferred for the purpose of assisting others in a bank robbery, and if that robbery occurs, the person providing the information is subject to accomplice culpability, even if he obtained the blueprint from a

textbook, from city hall, or from the newspaper. See also United States v. Edler Industries, Inc., 579 F.2d 516, 521 (9th Cir. 1978) (though the dissemination and export of technological information on how to manufacture military equipment otherwise might generally be protected by the First Amendment, there is no constitutional protection for export of such information as part of "the conduct of assisting foreign enterprises to obtain military equipment"); Constitutionality of the Proposed Revision of the International Traffic in Arms Regulations, 5 Op. O.L.C. 202, 206-09 (1981) (discussing Edler Industries).

In a number of cases, persons have been convicted of aiding and abetting violations of the tax laws by providing explicit instructions to a discrete group of listeners on techniques for avoiding disclosure of tax liability. See supra notes 23-24. Defendants in such cases often have invoked the First Amendment; but that constitutional guarantee has rarely, if ever, been a bar to accomplice culpability. The courts correctly have rejected defendants' reliance on Brandenburg; and, in particular, have refused to accept defendants' arguments that the "imminence" requirements of the Brandenburg test apply to such aiding and abetting cases. If a defendant has aided and abetted a crime through the dissemination of information -- rather than simply by urging or "advocating" that the crime be committed -- then the government should not need to demonstrate that the speech was intended or likely to "incite" imminent unlawful conduct. The reasons the strict requirements of the Brandenburg test must be applied to cases of advocacy are that (i) abstract advocacy of unlawful conduct usually is closely aligned with (or sometimes part of) political and ideological speech entitled to the strongest constitutional solicitude; and (ii) the danger the speech will in fact lead to unlawful behavior often is remote and speculative. These concerns are rarely, if ever, implicated, in cases involving conduct constituting intentional and material aid to the criminal conduct of particular persons. It follows that the question of whether criminal conduct is "imminent" is relevant for constitutional purposes only where, as in Brandenburg itself, the government attempts to restrict advocacy, as such. But the tax-avoidance aiding and abetting cases are not subject to Brandenburg because culpability in such cases is premised, not on defendants' "advocacy" of criminal conduct, but on defendants' successful efforts to assist others by detailing to them the means of accomplishing the crimes.⁶¹

If it were otherwise -- that is, if the Brandenburg test applied to crimes implemented through the use of informative speech -- there would, for example, be no way for the government to prohibit the aiding and abetting of a crime that is intended to occur weeks or months after its planning. But in fact, if someone in October teaches another person how to cheat on their tax forms to be filed the following April, the person doing the teaching nonetheless can be culpable of aiding and abetting tax fraud. "The fact that the aider and abettor's counsel and encouragement is not acted upon for long periods of time does not break the actual connection between the commission of the crime and the advice to commit it." United States v. Barnett, 667 F.2d 835, 841 (9th Cir. 1982).

Just as advocacy of unlawful conduct is entitled to greater constitutional protection than the act of using speech to aid and abet such conduct, Brandenburg itself recognizes another, related distinction that is of equal significance for present purposes. As we explained above, the Court in Brandenburg held that the First Amendment renders invalid statutes that "forbid or proscribe advocacy of the use of force or of law violation except where such advocacy is directed to inciting or producing imminent lawless action and is likely to incite or produce such action." 395 U.S. at 447. Immediately after stating this constitutional requirement, however, the Court drew a sharp distinction between "the mere abstract teaching . . . of the moral propriety or even moral necessity for a resort to force and violence" and "preparing a group for violent action and steeling it to such action." Id. at 448 (quoting Noto v. United States, 367 U.S. 290, 297-98 (1961)).

As the Court made plain in Noto and in related cases, the latter category of conduct -- "preparing a group

for violent action and steeling it to such action" -- is not entitled to First Amendment protection, even though advocacy ("the mere abstract teaching . . . of the moral propriety") of such violence is protected. Indeed, even Justice Douglas -- in the course of urging strong constitutional protection for the advocacy of illegality - - freely acknowledged that "[t]he freedom to speak is not absolute; the teaching of methods of terror . . . should be beyond the pale." Dennis v. United States, 341 U.S. 494, 581 (1951) (Douglas, J., dissenting) (emphasis added).

The distinction recognized in Brandenburg between advocacy of, and preparation for, unlawful conduct, was exemplified in Scales v. United States, 367 U.S. 203 (1961), a case in which the Court carefully distinguished between the teaching of abstract doctrine -- punishment of which is subject to substantial constitutional constraints -- and the teaching of the techniques of unlawful conduct, which can much more easily be proscribed. Id. at 233-34. As to the former, the Court has developed the Brandenburg test, which asks whether the danger is intended, likely and "imminent." But the constraints of the First Amendment do not apply when the "teaching" goes "beyond the theory itself" to "an explanation of `basic strategy.'" Scales, 367 U.S. at 244. At that point, the teaching -- if it is done with the purpose of preparing a group for unlawful action -- is not much different than the information conveyed in a typical aiding and abetting case; accordingly, the Brandenburg protections should largely be inapposite. See Yates v. United States, 354 U.S. 298, 331-33 (1957) ("systematic teaching" in classes to "develop in the members of [a] group a readiness to engage [in unlawful conduct] at the crucial time," could be punished, even if that conduct was to occur only "when the time was ripe").⁶²

This critical distinction -- between advocacy of unlawful conduct, on the one hand, and "instructions" for unlawful conduct, on the other -- was recognized by Professor Thomas Emerson in his seminal treatise on the First Amendment:

[C]onduct that amounts to "advice" or "persuasion" [sh]ould be protected; conduct that moves into the area of "instructions" or "preparations" [sh]ould not. The essential task would be to distinguish between simply conveying an idea to another person, which idea he may later act upon, and actually participating with him in the performance of an illegal act. It is true that the distinction does not offer automatic solutions and that courts could easily disagree on any particular set of facts. But this process of decision making is related to the nature of "expression" and the functions and operations of a system of freedom of expression. It is therefore a rational method of approaching the problem.

Thomas Emerson, The System of the Freedom of Expression 75 (1970).⁶³

B. Application of First Amendment Principles to Dissemination of Bombmaking Information

Having reviewed the role of the First Amendment in these three related contexts, we now can address specifically the circumstances under which Senators Feinstein and Biden would seek to proscribe dissemination of bombmaking information.

1. Dissemination with the "Intent" to Facilitate Unlawful Conduct. The Feinstein Amendment would make it unlawful, inter alia, for any person to "teach or demonstrate" the making of explosive materials, or to distribute by any means information pertaining to, in whole or in part, the manufacture of explosive materials, where the person "intend[ed]" that such information would be used for, or in furtherance of, an activity that "constitutes a Federal criminal offense or a criminal purpose affecting interstate commerce." In light of the foregoing discussion in Part VI-A, two things about the constitutionality of this "intent" prohibition are clear:

First, the First Amendment almost certainly would require that the "intent" scienter provision in such a statute be construed to mean an actual, conscious purpose to bring about the specified result. "Intent" may not be construed as "constructive intent," as in the civil tort context; that is to say, "intent" could not constitutionally be inferred solely by virtue of the fact that criminal offenses were a foreseeable result -- a "natural consequence" -- of the general distribution of bombmaking information. Anyone who teaches or publishes bombmaking information -- including those who do so for wholly legitimate reasons, such as explosives manufacturers, the military, and encyclopedia publishers -- could foresee that some unknown recipient of the teaching or information will use it for unlawful ends; but the First Amendment would not permit culpability on that basis. See supra at 30-34. Instead, an "intent" element must be construed to reach only the person who disseminates the information for the purpose of facilitating criminal conduct.⁶⁴

Second, a prosecution relying upon an "intent" requirement plainly would be constitutional where the teacher intends that a particular student -- or a discrete group of students -- use the information for criminal conduct. Indeed, if there is such an intent, and a receiver of the information thereafter does use that information to commit a crime, the person who assisted him by showing him how to do so would be culpable as an aider and abettor, and the First Amendment would not bar such accomplice culpability. See supra at 36-39. The constitutional analysis should be the same, as in the Featherston case, where the teacher intends that particular students use the information for unlawful ends, but the crime is never committed (such as when the scheme is foiled by detection). This would be, in essence, a form of "attempted aiding and abetting." Although presently there is no general federal statute prohibiting "attempted aiding and abetting," see supra at 20, that is not because of any constitutional bar: application of such a statute to the provision of information would not transgress the First Amendment. Therefore, a statute like the Feinstein Amendment could constitutionally be applied to a case where the person supplying the critical training or information has the intent thereby to assist a particular recipient thereof in unlawful activity, whether or not the crime eventually occurs.⁶⁵ As the Court emphasized in Brandenburg and in earlier cases, the Constitution does not protect the conduct of "preparing a group for violent action" by teaching the techniques of unlawful conduct. See Noto; Scales; Dennis, 341 U.S. at 581 (Douglas, J., dissenting); Emerson, System of Freedom, supra, at 75; Greenawalt, Speech, Crime, supra note 20, at 244-45.⁶⁶

The more difficult question is whether criminal culpability can attach to general publication of explosives information, when the writer, publisher or seller of the information has the purpose of generally assisting unknown and unidentified readers in the commission of crimes. This is, in essence, the situation alleged in the recent Rice v. Paladin case. See supra at 27-28. To be sure, such a "generalized" attempt to aid crime through publication is "not the same as preparing a group for violent action." Noto, 367 U.S. at 298. The "joint participation" in a crime that is the hallmark of conspiracy or aiding and abetting is absent here: the speech is not, in any direct sense, "brigaded with action." What is more, the danger to the public in such a case is not necessarily greater than that caused by the same exact publication that is made solely for permissible purposes. The constitutional question is, therefore, more difficult than in the case of intentional concerted action discussed above.

There are few, if any, cases directly on point.⁶⁷ However, in Haig v. Agee, 453 U.S. 280 (1981), the Court suggested that otherwise privileged publication of information can lose its First Amendment protection when the publisher has an impermissible motive. In Agee, a former CIA employee had his passport revoked as a result of his campaign to publish the names of (and otherwise publicly identify) intelligence agents working in foreign countries, a course of conduct that undermined intelligence operations and endangered agents. In the context of this serious threat to American national security, the Court held that the First Amendment did not protect Agee's publication of the agents' names. In so ruling, the Court stressed the following:

Agee's disclosures, among other things, have the declared purpose of obstructing intelligence operations and the recruiting of intelligence personnel. They are clearly not protected by the Constitution. The mere fact that Agee is also engaged in criticism of the Government does not render his conduct beyond the reach of the law.

Id. at 308-09 (emphasis added). The Court did not indicate whether Agee's bad intent was, in and of itself, sufficient to strip his speech of its constitutional protection. In particular, the Court had no occasion to determine whether the First Amendment analysis would be the same if the information Agee published was already in the public domain and/or if the government's interests were not as significant as the protection of intelligence sources.

Nonetheless, in the absence of contrary authority, this passage in Haig v. Agee supports the argument that the government may punish publication of dangerous instructional information where that publication is motivated by a desire to facilitate the unlawful use of explosives.⁶⁸ At the very least, publication with such an improper intent should not be constitutionally protected where it is foreseeable that the publication will be used for criminal purposes; and the Brandenburg requirement that the facilitated crime be "imminent" should be of little, if any, relevance.⁶⁹ Accordingly, we believe that the district court in Rice v. Paladin, seesupra at 27-28, erred insofar as it concluded that Brandenburg bars liability for dissemination of bombmaking information regardless of the publisher's intent. See also infra note 71.

Having said that, we should note that where there is no concerted action between the publisher and any particular recipient of the information, there might be a significant problem in proving that the person publishing the information has done so with an impermissible purpose. Most publishers of the bombmaking materials in question will argue that their publication is well-intentioned. For example, in Rice, the publisher of Hit Man has asserted that its intended audience includes: authors who desire information for the purpose of writing books about crime and criminals; law enforcement officers and agencies who desire information concerning the means and methods of committing crimes; persons who enjoy reading accounts of crimes and the means of committing them for purposes of entertainment; persons who fantasize about committing crimes but do not thereafter commit them; and criminologists and others who study criminal methods and mentality. See supra at 28.

Nevertheless, proof of improper intent might be possible in certain types of cases. In many cases the manuals themselves might have "the declared purpose," Agee, 453 U.S. at 309, of facilitating crime. Although, under Brandenburg, culpability cannot attach merely because the manuals advocate unlawful action, such advocacy could constitutionally be used as probative evidence that the disseminator of accompanying information on the techniques of bombmaking intended by such dissemination to facilitate criminal conduct. See supra note 47. What is more, if a publisher of such communications engages in a marketing strategy intended to maximize sales to, inter alia, "criminals and would-be criminals who desire

information and instructions on how to commit crimes," as the publisher of Hit Man allegedly did, and if that publisher's economic success evidently depends upon stimulating a high volume of unlawful use of his product -- i.e., the publisher's fortunes substantially rise or fall depending on the degree to which his product facilitates unlawful conduct -- there might be sufficient evidence of improper intent. See Direct Sales, 319 U.S. at 712-13 (where seller of dangerous drugs -- which could be used both for proper and improper purposes -- engaged in marketing strategy to stimulate sales to would-be criminals, and where seller had a "stake in the venture," it was permissible to infer intent to assist criminal operation). As Justice Holmes explained in a related context, it is fair to assume that items are "designed for" unlawful use where they are "offered for sale in such a mode as purposely to attract purchasers who wanted them for the unlawful [use]." Danovitz v. United States, 281 U.S. 389, 397 (1930).

Finally, if, as Senator Feinstein believed, some of the information contained in the bombmaking manuals has no use other than to facilitate unlawful conduct,⁷⁰ that fact, too, would be evidence of an intent to facilitate crime (at least with respect to that particular information). Publishers of such information undoubtedly would argue that such information has uses other than to facilitate unlawful conduct -- such as to educate law enforcement officials and would-be murder-mystery writers, and simply to entertain persons who enjoy reading accounts of the workings of the criminal mind. See supra at 28 (describing claims made by publisher of Hit Man). But that assertion would only raise, rather than resolve, the critical question of fact regarding a publisher's intent; it would remain an issue for the trier of fact to determine whether one of the publisher's purposes was to facilitate criminal conduct.

We acknowledge that in many cases, there may be a broad and diverse audience for such communications, including persons who would not use the information as a blueprint for crime, and the communications might have substantial value other than to facilitate crimes. In such cases, courts might agree that "a strict rule about finding intent is especially important, lest a jury convict because of outrage over the facts someone has chosen to disclose. A person should not be punished for encouraging a general crime like murder by publicly disclosing facts unless the prosecution's evidence leaves no possible doubt that his purpose has been to aid or cause that criminal result." Greenawalt, Speech, Crime, supra note 20, at 273. But where such a purpose is proved beyond a reasonable doubt, as it would have to be in a criminal case, the First Amendment should be no bar to culpability.⁷¹

2. Dissemination with the "Knowledge" that a Particular Recipient of the Information Intends to Use It in Furtherance of Unlawful Conduct. The Feinstein Amendment also would have made it unlawful, inter alia, for any person to "teach or demonstrate" the making of explosive materials, or to distribute by any means information pertaining to, in whole or in part, the manufacture of explosive materials, if the person "knows" that such information will be used for, or in furtherance of, "an activity that constitutes a Federal criminal offense or a criminal purpose affecting interstate commerce." As Senator Biden explained, this "knowledge" provision was intended to address the case where the person disseminating the information has evidence that a particular potential recipient plans to use that information to engage in unlawful activities -- for example, when the person requesting the information expressly indicates that he plans to use the information to learn how to commit violent crimes. See supra note 38.

It is questionable whether the statutory scienter requirement ("knows") in the Feinstein Amendment would suffice to cover such a situation. As explained above, supra at 21 & note 32, where a statutory element of "knowledge" refers to a possible future result of a defendant's conduct, the government typically must prove that the defendant was "aware that that result is practically certain to follow from his conduct." United States v. Bailey, 444 U.S. 394, 404 (1980) (citations omitted). Thus, even where someone expressly states

that he desires to purchase a product in order to plan a crime, it might be difficult to persuade the trier of fact that it was "practically certain" that the crime would be committed (particularly if, as it turned out, the crime was not in fact committed). It would, therefore, be helpful to identify a more carefully tailored mens rea requirement in order to address Senator Biden's hypothetical situation.

The scenario Senator Biden describes brings to mind other types of "facilitation" statutes, such as state statutes making it a crime to "provide" a person with "means or opportunity" to commit a crime, "believing it probable that he is rendering aid to a person who intends to commit a [crime]." N.Y. Penal Law § 115.05 (McKinney 1996).⁷² Such statutes, however, are of general applicability: they do not single out a particular form of facilitation, such as facilitation involving conveyance of information, for especially harsh treatment. And what is more, conviction under such statutes -- as under the federal aiding and abetting statute, 18 U.S.C. § 2 -- requires that the facilitation actually result in the commission of a crime.⁷³

A closer analogy, therefore, might be another section of the AEDPA itself. Section 706 of the AEDPA makes it a felony to "knowingly transfer[] any explosive materials, knowing or having reasonable cause to believe that such explosive materials will be used to commit a crime of violence . . . or drug trafficking crime." 110 Stat. at 1295-96 (to be codified at 18 U.S.C. § 844(o)).⁷⁴ The "reasonable cause to believe that [the item] will be used [for the unlawful purpose]" standard would seem to address directly the case where the recipient of the product indicates an intent to use it to commit or to facilitate a crime. The constitutional question then becomes whether such a standard can be used where the item being transferred is not "explosive materials," as in AEDPA section 706, but instead information on how to manufacture or use such materials.

There is little case law directly on point. As Professor Greenawalt points out, however, this case is not quite as easy from a First Amendment perspective as "attempted aiding and abetting," which can constitutionally be proscribed because it requires a specific purpose to actually assist in the commission of the crime:

It is only a minor impairment of freedom to tell people they cannot provide information they want to be used for a crime. It is somewhat more serious to tell them that, even if they have no such purpose, they must keep their mouths shut. A speaker may conceivably think a communication has significant value for the listener beyond the listener's immediate purpose, but, even if the speaker does not think that, perhaps a recognition of the speaker's autonomy should include allowing him ordinarily to say what he believes to be true to his acquaintances, regardless of the use he thinks they plan to make of it.

A further argument against such liability is the problem of determining facts accurately and the effect of the resulting uncertainty on people who speak. If people become aware that they can be treated as criminal for providing information they believe will aid a crime, they may hesitate to give information when they think there is some modest chance of criminal use, not trusting that prosecutors and jurors will always be discerning about

perceptions of relevant probabilities.

The implications for free speech are serious enough to warrant careful attention to the problem of communications that facilitate.

Greenawalt, Speech, Crime, supra note 20, at 86-87.

There are two principal reasons why a "facilitation through speech" prohibition without an "intent" requirement would raise serious First Amendment problems. First, such a facilitation prohibition would be directed specifically and uniquely at facilitation effected by way of conveying information. In other words, it would not prohibit facilitation, as such, but only a speech-related subset of such conduct. "The text of the First Amendment makes clear that the Constitution presumes that attempts to regulate speech are more dangerous than attempts to regulate conduct." 44 Liquormart, Inc. v. Rhode Island, 116 S. Ct. 1495, 1512 (1996) (plurality opinion). The constitutionality of the prohibition therefore is not as clear as it would be if "facilitation through speech" were just one form -- i.e., one application -- of a generally applicable facilitation statute that did not refer specifically to speech. See Cohen v. Cowles Media Co., 501 U.S. 663, 669-71 (1991) (whereas First Amendment is not implicated by application of "generally applicable laws" to violations involving speech or the press, there is a greater constitutional problem where, as in Florida Star, the "State itself define[s] the content of publications that would trigger liability").

Second, as explained above, supra at 30-34, the First Amendment traditionally has been understood to prohibit the use of the criminal or tort law to punish the dissemination of lawfully obtained factual information absent an impermissible purpose for such dissemination; and this is so even where such publication has a "propensity" to be misused by someone in a criminal or tortious manner. Yet that is, in a sense, precisely what a facilitation prohibition would do in Senator Biden's scenario: it would punish distribution of lawfully obtained information because the disseminator had reason to believe that such distribution would result in some harm.

Although the matter is far from certain, in the end we think these First Amendment concerns can be overcome, and that such a facilitation prohibition could be constitutional, if drafted narrowly. To be sure, the prohibition would be "speech-specific." But, as with respect to 18 U.S.C. § 231(a)(1), see supra at 21-23, Congress would be singling out "teaching" and "informational" facilitation of crime not because of any hostility to speech itself, but because those are the forms of facilitation that are the most apparent threats to safety not already addressed by accomplice and conspiracy prohibitions and by the facilitation prohibitions found in sections 323 and 706 of the AEDPA. Congress arguably would simply be filling in a statutory gap, rather than expressing a general hostility to any particular viewpoint. Accordingly, the constitutional problems should be minimized. See Edler Industries, 579 F.2d at 520-22 (whereas First Amendment would prohibit export restrictions dealing with general "interchange of scientific and technological information," it is constitutional to restrict such export where the exporter knows or has reason to know that the recipient of the information will use it to produce or operate munitions). See also Constitutionality of the Proposed Revision of the International Traffic in Arms Regulations, 5 Op. O.L.C. 202, 207-08 (1981).

Furthermore, such a prohibition could be, in constitutionally significant respects, less problematic than a statute or tort that punishes speech having a propensity to be misused by some unknown recipient. In the latter type of tort and criminal cases, the practical effect of a penalty would be to deter altogether the dissemination of the information, since there is always a chance that some reader, listener or viewer will turn

the information to bad use, and the only way to avoid this risk is to cease speaking altogether. Indeed, even where there would in fact be only a slim likelihood that the information would be misused, a jury might be expected to find the requisite degree of "recklessness," particularly if -- as is likely in such cases -- the jury is hostile to the message conveyed in the information and does not believe that it serves any social utility to distribute such information. The risk of such an outcome effectively could chill the "legitimate" dissemination of bombmaking information even if there is but a slight risk of its misuse.⁷⁵ By contrast, a facilitation prohibition tailored to particular recipients who are likely to make criminal use of the information would not have such a broad chilling effect on such speech. The person conveying the information would be required only to withhold its distribution to particular persons who pose an apparent risk, and otherwise would be able to continue general publication, distribution or sales. In other words, such a prohibition would only restrict or deter certain particular transactions, but would not impede general publication.

In drafting a constitutional facilitation statute, we think the safest strategy would be to address Senator Biden's scenario directly -- for example, by barring dissemination of bomb-making information to a particular person, where the disseminator knows that such person intends to use the information for an unlawful purpose. Under such a statute, the requisite "knowledge" would not be of a future event, but instead, of someone else's present intent. Therefore, the government would not be required to prove that the disseminator was "practically certain" of the recipient's intent. See supra at 21 (discussing "practical certainty" standard for "knowledge" of future events). Instead, it should suffice to prove that the person providing the information was aware of a "high probability" that the recipient had an intent to use the information to commit a crime. See, e.g., Barnes v. United States, 412 U.S. 837, 845 (1973); Turner v. United States, 396 U.S. 398, 416 & n.29 (1970); Leary v. United States, 395 U.S. 6, 46 n.93 (1969).⁷⁶ That "knowledge" typically should be found where, as in the cases hypothesized by Senator Biden, the recipient clearly indicates to the disseminator a desire to use the information for criminal purposes.⁷⁷

Alternatively, Congress could decide to track the language of section 706 of the AEDPA, such as the following:

It shall be unlawful for any person to teach or demonstrate to any particular person the making of explosive materials,
 or to distribute to any particular person, by any means, information pertaining to, in whole or in part, the manufacture of
 explosive materials, with reasonable cause to believe that such particular person will use such teaching, demonstration
 or information for, or in furtherance of, an activity that constitutes a Federal criminal offense or a criminal offense
 affecting interstate commerce.

That formulation would almost certainly cover the case where the recipient of the information expressly indicates an intent to use such information to commit or to facilitate a crime, and would likely be constitutional as applied to such a case. However, such a "reasonable cause to believe" standard might also deter widespread, general publication of such information where a publisher is aware that certain suspicious persons are in the "audience."⁷⁸ Because of this risk of chilling substantial publication of such information to persons who will not use it unlawfully, such a statute would run a greater risk of constitutional invalidation than a statute (such as that described above) that is more narrowly tailored to the particular hypothetical described by Senator Biden.⁷⁹

C. Proposed Modification of the Feinstein Amendment

For the reasons discussed in the preceding sections, the Feinstein Amendment would be more likely to reach all of the fact situations that Senators Feinstein and Biden wished to address, and would be more likely to pass constitutional muster in most or all of its applications, if it were modified to read as follows:

It shall be unlawful for any person --

(a) to teach or demonstrate the making or use of an explosive, a destructive device, or a weapon of mass destruction, or to

distribute by any means information pertaining to, in whole or in part, the manufacture or use of such an explosive, device or

weapon, intending that such teaching, demonstration or information be used for, or in furtherance of, an activity that

constitutes a Federal criminal offense or a State or local criminal offense affecting interstate commerce,⁸⁰ or

(b) to teach or demonstrate to any particular person the making or use of an explosive, a destructive device, or a weapon of

mass destruction, or to distribute to any particular person, by any means, information pertaining to, in whole or in part, the

manufacture or use of such an explosive, device or weapon, knowing that such particular person intends to use such

teaching, demonstration or information for, or in furtherance of, an activity that constitutes a Federal criminal offense or State

or local criminal offense affecting interstate commerce.

For purposes of this section, the term "explosive" has the meaning set out in 18 U.S.C. § 844(j). The term "destructive

device" has the meaning set out in 18 U.S.C. § 921(a)(4). The term "weapon of mass destruction" has the meaning set out in

18 U.S.C.A. § 2332a(c)(2).

The principal differences between this proposal and the Feinstein Amendment itself are the following:

1. The Feinstein Amendment could be construed to impose culpability if the person disseminating the information has reason to know that some unidentified, unspecified recipient thereof will use the information for an unlawful purpose, or if such an outcome is the "natural consequence" of publication of the information. Because that construction could cover virtually all public dissemination of such information, it would raise serious constitutional questions. The alternative formulation specifies that the person who disseminates the information must either have the specific purpose of facilitating criminal conduct, or must have knowledge that a particular recipient intends to make improper use of the material. This should, for example, address Senator Biden's example of a sale of a bombmaking manual to a purchaser who has requested it for the express purpose of using such information to accomplish an unlawful end. In such a case, a well-intentioned distributor of the information will be prohibited from providing the information to the requesting party, but may otherwise freely offer the item for sale.

2. Under the Feinstein Amendment, it would be unclear whether criminal culpability would attach where

someone disseminates dangerous information about explosives with a conscious purpose of facilitating unlawful conduct by unknown recipients of the information. The alternative formulation would make clear that dissemination with such a specific purpose would be proscribed. While the constitutionality of particular applications of such a prohibition might be somewhat uncertain (depending on whether the evidence truly demonstrates the improper intent beyond a reasonable doubt), we believe that the "intent" prohibition would be facially constitutional.⁸¹

3. The alternative formulation would make clear that the "intent" or "knowledge" element refers to the use made of the information that the person disseminates. Accordingly, it does not include the Feinstein Amendment's language regarding "such explosive materials," because that phrase did not have a clear referent: the prohibition should involve dissemination or teaching of information, not dissemination of the explosive materials themselves (which is independently addressed elsewhere in Title 18 and in the AEDPA).

4. The alternative formulation would broaden the Feinstein Amendment to bring within its ambit teaching and information concerning not only explosives (as defined in 18 U.S.C. § 844(j)), but also all destructive devices (as defined in 18 U.S.C. § 921(a)(4)) and other weapons of mass destruction (as defined in 18 U.S.C.A. § 2332a(c)(2)).

5. The alternative formulation would broaden the Feinstein Amendment to cover information about the "use" of explosives, in addition to the manufacture thereof. In the wrong hands, information on how to use explosives (such as the information in Hit Man that was used to commit a multiple homicide, discussed in Rice v. Paladin) can be every bit as dangerous as information on how to create such explosives.

6. For purposes of clarification and simplicity, the alternative formulation refers to a "State or local criminal offense affecting interstate commerce," rather than to a "criminal purpose affecting interstate commerce." It is unclear how a "criminal purpose" could "affect" interstate commerce.

ENDNOTES:

¹ See Statement of Robert S. Litt, Deputy Assistant Attorney General, Criminal Division, U.S. Department of Justice, in Mayhem Manuals and the Internet: Hearings Before the Subcomm. on Terrorism, Technology and Government Information of the Senate Comm. on the Judiciary, 104th Cong., 1st Sess. (1995).

² The DOJ Committee considered carefully the question whether the inclusion in this Report of titles of, and illustrative excerpts from, bombmaking texts would enhance the availability of such information to persons bent upon fabricating bombs and other destructive devices. The Committee concluded that such information already is so readily available to such individuals that its publication in a Report to Congress will create no additional risk. Nevertheless, except as specifically noted, the mention of any particular source of bombmaking information in this Report should not be taken as validation or acknowledgement of the accuracy or value of that information.

³ See also infra note 54 (discussing publication by various periodicals, including the Progressive, of articles describing technical processes of thermonuclear weapons).

⁴ See "Hunt for a Mad Bomber," Reader's Digest 77, 79 (August 1993).

⁵ Much of the information available in print pertaining to nuclear weapons also can be found on the Internet. A number of websites, for example, have included compilations of nuclear weapons information gleaned from literature elsewhere in the public domain.

⁶ The list, captioned "Bombs: All About Things that Go Boom," includes a warning that the compiler does "not endorse, nor check for

the safety, or validity of these bomb making procedures. Makers of these devices take all responsibility. . . . [A]ll of these devices do or can pose a risk to the creators and other individuals." The compiler further suggests that "[f]or [the reader's] safety please read the recipes carefully two and three times over before attempting."

It is important to note that, even if a user of the World Wide Web does not know the specific location of a website containing bombmaking information, such data can easily be located with a search engine.

⁷ In a colloquy during the Senate's consideration of the Feinstein Amendment, see supra at 3-4, Senators Biden and Feinstein described similar material that members of their staffs had obtained over the Internet. Senator Biden referred to one item that instructed readers how to manufacture a "baby food bomb" from shotgun shells and "other materials that can be obtained by anyone" that are so "powerful that they can destroy a car." 142 Cong. Rec. S3448 (daily ed. Apr. 17, 1996) (statement of Sen. Biden). Senator Feinstein observed that The Terrorist's Handbook is available by mail order and on the Internet. She observed that this book begins by stating that "[w]hether you are planning to blow up the World Trade Center, or merely explode a few small devices on the White House lawn, the 'Terrorist's Handbook' is an invaluable guide to having a good time." It then goes on to explain, among other things, how to steal the chemicals necessary for making an explosive from a college laboratory. 142 Cong. Rec. S7272 (daily ed. June 28, 1996) (statement of Sen. Feinstein).

⁸ All three defendants were convicted by jury on April 24, 1996, on charges that included conspiracy to make a destructive device to be used to destroy a building used in interstate commerce.

⁹ In 1995, all four members were subsequently tried, convicted and sentenced for violating 18 U.S.C. § 175 (unlawful possession of biological weapons). Although the Patriot Council members only possessed 0.7 grams of ricin, this minute amount constitutes more than 100 lethal doses.

We note that, on November 1, 1995, a senior official of the FBI, testifying before the Senate Permanent Subcommittee on Investigations, apprised the Subcommittee members of the ricin plot, including the use by the conspirators of a publicly available instruction manual describing manufacture of the toxic poison. See Statement of John P. O'Neill, Chief, Counterterrorism Section, FBI, in Global Proliferation of Weapons of Mass Destruction: Hearings Before the Permanent Subcomm. on Investigations of the Senate Comm. on Governmental Affairs, 104th Cong., 1st Sess. 236 (1995). Another senior FBI official furnished identical information to the House Subcommittee on Military Research and Development. See Statement of Robert M. Blitzer, Chief, Domestic Terrorism/Planning Section, FBI, in Chemical-Biological Defense Program and Response to Urban Terrorism: Hearings Before the Subcomm. on Military Research and Development of the House Comm. on National Security, published at 1996 WL 7136609 (Mar. 12, 1996).

¹⁰ See also Department of the Treasury, Bureau of Alcohol, Tobacco and Firearms, Arson and Explosives -- Incidents Report 1994, at 41-51 (1995).

¹¹ This Report deals almost exclusively with the ability of the government to prohibit or restrict the dissemination by private persons of bombmaking information that has not been classified. The Report does not discuss in any detail the separate, broader authority of the government to impose "reasonable restrictions" on its own employees' activities to ensure that those employees do not disclose classified information belonging to the government itself. See generally Snepp v. United States, 444 U.S. 507 (1980).

¹² With respect to information concerning atomic weapons in particular, there is another restriction in federal law that also should be mentioned. The Atomic Energy Act imposes certain restrictions on the dissemination of "Restricted Data," which is defined to include, inter alia, "all data concerning design, manufacture, or utilization of atomic weapons," 42 U.S.C. § 2014(y)(1), unless such information has been expressly "declassified or removed from the Restricted Data category," id. In particular, it is unlawful to communicate, transmit or disclose such "Restricted Data" to any person either (i) with intent to injure the United States or with intent to secure an advantage to any foreign nation, 42 U.S.C. § 2274(a), or (ii) with "reason to believe such data will be utilized to injure the United States or to secure an advantage to any foreign nation," id. § 2274(b). In addition, the Attorney General may apply to a court for an injunction prohibiting impermissible dissemination of such Restricted Data by persons who are "about to engage" in such conduct. 42 U.S.C. § 2280.

Insofar as Restricted Data includes simply information produced by or for the government -- such as the government's self-generated, classified information -- the extent to which the government may prohibit dissemination of such data by those who are granted access to it is a matter outside the principal scope of this Report. See supra note 11; infra note 44. However, there is a serious

question whether Restricted Data also includes information developed or compiled by private citizens who have not had access to classified government documents. See generally Mary M. Cheh, The Progressive Case and the Atomic Energy Act: Waking to the Dangers of Government Information Controls, 48 Geo. Wash. L. Rev. 163, 180-88 (1980). The position of the Department of Energy is that such "privately generated" information concerning nuclear weapon design can be Restricted Data subject to the statutory restrictions on dissemination, see 62 Fed. Reg. 2252, 2254, 2261 (Jan. 15, 1997) (proposing new 10 C.F.R. § 1045.21, which would make this point explicitly); and the only court to opine on the matter has confirmed this statutory construction, see United States v. Progressive, Inc., 467 F. Supp. 990, 998-1000 (W.D. Wis.), rehearing denied, 486 F. Supp. 5 (W.D. Wis.), appeal dismissed, 610 F.2d 819 (7th Cir. 1979). Insofar as the Restricted Data provisions do encompass certain privately generated information concerning nuclear weapons, see 62 Fed. Reg. at 2253-54 (discussing the types of information that the Department of Energy presently considers Restricted Data), the Atomic Energy Act would provide another statutory means of limiting the dissemination of such forms of bombmaking information. However, because Senator Feinstein's initiative in the last Congress was not directed specifically to information about such nuclear weapons, we will limit our discussion of Restricted Data to this footnote, except to note the following: As discussed infra at 30-34 & note 54, any attempt by the government to restrict or punish the dissemination of Restricted Data that was already in the public domain would run up against significant First Amendment constraints, absent an intent by the disseminator to injure the United States or to secure an advantage to any foreign nation.

¹³ Cf., e.g., United States v. Rowlee, 899 F.2d 1275, 1278 (2d Cir.) (defendant properly convicted of conspiracy to defraud United States based on having provided instruction and assistance to others in avoiding income tax liability), cert. denied, 498 U.S. 828 (1990); United States v. Daly, 756 F.2d 1076, 1081-82 (5th Cir. 1985) (defendant properly convicted of conspiracy to defraud United States based on having disseminated information to members of church on how to file tax returns so as to hamper IRS investigation).

¹⁴ See, e.g., United States v. Donner, 497 F.2d 184, 192 (7th Cir. 1972) (speech, including otherwise constitutionally protected speech, can constitute overt act in furtherance of conspiracy), cert. denied, 419 U.S. 1047 (1974).

¹⁵ See generally Direct Sales Co. v. United States, 319 U.S. 703 (1943); United States v. Falcone, 311 U.S. 205 (1940); United States v. Pinckney, 85 F.3d 4, 8 (2d Cir. 1996).

¹⁶ See Direct Sales; Falcone; United States v. Blankenship, 970 F.2d 283 (7th Cir. 1992).

¹⁷ See also Lechuga, 994 F.2d at 349-50 (opinion for four judges of 11-member en banc panel); id. at 362-63 (opinion of three other judges, concurring on this point). However, where the commodity in question has an "inherent capacity" to be used unlawfully, and where the provider of the product has a stake in the success of the illegal venture for which that product is used, a regular course of conduct involving such sales may support proof of a conspiracy. Direct Sales, 319 U.S. at 711-13.

¹⁸ See, e.g., United States v. McNeill, 887 F.2d 448, 450-52 (3d Cir. 1989), cert. denied, 493 U.S. 1087 (1990).

¹⁹ Similarly, the First Amendment does not protect an offer to engage in an unlawful transaction or activity. See, e.g., Village of Hoffman Estates v. Flipside, Hoffman Estates, Inc., 455 U.S. 489, 496 (1982); Pittsburgh Press Co. v. Pittsburgh Comm'n on Human Relations, 413 U.S. 376, 388 (1973); Braun v. Soldier of Fortune Magazine, Inc., 968 F.2d 1110, 1116-21 (11th Cir. 1992), cert. denied, 506 U.S. 1071 (1993); Norwood v. Soldier of Fortune Magazine, Inc., 651 F. Supp. 1397, 1398-1402 (W.D. Ark. 1987).

²⁰ See District of Columbia v. Garcia, 335 A.2d 217, 224 (D.C.) (distinguishing between constitutionally protected advocacy and "the act of enticing or importuning on a personal basis for personal benefit or gain"), cert. denied, 423 U.S. 894 (1975). See also People v. Rubin, 158 Cal. Rptr. 488, 491 (Cal. Ct. App. 1979) (discussing distinction between "general advocacy of crime" and solicitation of crime accompanied by "offer of reward"), cert. denied, 449 U.S. 821 (1980). Professor Kent Greenawalt has argued that the Brandenburg requirements (such as the requirement of "imminent" criminal conduct) should be relaxed in the case of private, nonideological solicitations to crime, even where there is no inducement or threat, but only persuasion. Kent Greenawalt, Speech, Crime, and the Uses of Language 261-65 (1989). While this argument has some force, we are not aware that any court has yet endorsed it.

²¹ See, e.g., United States v. Razo-Leora, 961 F.2d 1140, 1147 (5th Cir. 1992).

²² Subsection 2(a) reads: "Whoever commits an offense against the United States or aids, abets, counsels, commands, induces or procures its commission is punishable as a principal." This statute does not create a distinct federal offense; rather, it merely abolishes

the common-law distinction between principals and accessories. United States v. Superior Growers Supply, Inc., 982 F.2d 173, 177-78 (6th Cir. 1992).

²³ See, e.g., United States v. Kelley, 769 F.2d 215, 216-17 (4th Cir. 1985) (defendant aided and abetted tax fraud by instructing others on how to prepare false forms); United States v. Buttorff, 572 F.2d 619, 623 (8th Cir.) (same), cert. denied, 437 U.S. 906 (1978).

²⁴ The law is unsettled on the question of how much contact, or "proximity," is required between the principals and the accomplice -- that is to say, to what extent the accomplice must "know" who it is he is aiding. In a series of cases similar to those cited supra note 23, courts have found that defendants could be held culpable for aiding and abetting tax-code violations merely by virtue of having provided instruction on unlawful tax-fraud techniques to a discrete group of listeners who had indicated a specific interest in violating the law. See also, e.g., United States v. Rowlee, 899 F.2d 1275 (2d Cir.), cert. denied, 498 U.S. 828 (1990); United States v. Freeman, 761 F.2d 549 (9th Cir. 1985), cert. denied, 476 U.S. 1120 (1986); United States v. Daly, 756 F.2d 1076 (5th Cir. 1985); United States v. Moss, 604 F.2d 569 (8th Cir. 1979), cert. denied, 444 U.S. 1071 (1980). manufacture phencyclidine. The facts alleged in the search warrant established that Barnett provided essential information for the specific purpose of assisting Hensley in the commission of a crime.

A harder question is whether aiding and abetting can be established with even less direct connection between the aider and the principals. In Buttorff, the court of appeals held that the aiding and abetting "joint participation" test was satisfied by virtue of tax-evasion instructions that defendants had provided at "large public gatherings," presumably to persons whom they did not personally meet. 572 F.2d at 622-23. United States v. Barnett, 667 F.2d 835 (9th Cir. 1982), suggests that this same theory of aiding and abetting could be applied to written instructions sent by mail to a customer whom the publisher had never met. In that case, the defendant allegedly advertised in a magazine that it was making available for mail-order purchase a catalog of instructions for manufacture of phencyclidine, and sent such instructions -- along with the name of a "reliable" chemical supplier -- to a person who submitted the required \$10 purchase price. Id. at 840. In the context of determining whether there was probable cause for a warrant to search the seller's premises, the court held that these allegations were sufficient to allege that the publisher had aided and abetted the recipient's manufacture of phencyclidine. The court reasoned that:

[I]t is unnecessary for the government to show that Barnett [the seller of the instructions] ever met with Hensley [the buyer] in order to prove that he aided and abetted him in his attempt to manufacture phencyclidine. The facts alleged in the search warrant established that Barnett provided essential information for the specific purpose of assisting Hensley in the commission of a crime.

Id. at 843. (The opinion does not indicate whether the "facts alleged" in the search warrant included more than what is described above.)

By contrast, part of the aiding-and-abetting rationale in Buttorff and Barnett may have been implicitly questioned in Superior Growers. In that case, the Sixth Circuit held that an indictment had not adequately charged conspiracy to aid and abet marijuana possession against proprietors of a garden-supply store. The indictment alleged, inter alia, that the defendants "occasionally provided information and advice on how to grow marijuana to various customers"; but there was no allegation that any particular customer in fact used such advice to commit a crime. The court held that the "providing information" allegation "ultimately falls short" of alleging the requisite intent to aid and abet, "because it does not state that the publications or information were given with defendants' knowledge that a particular customer was planning to grow marijuana, and with defendants' intent to assist that customer in the endeavor." 982 F.2d at 178. According to the court, in other words, it was insufficient for the government merely to demonstrate that the proprietors intended to aid and abet their customers; it was essential to prove that the proprietors had knowledge that their customers were manufacturing marijuana "or intended to manufacture marijuana." Id. at 175.

²⁵ This standard applies even where the federal crime being assisted involves the unlawful use of explosives. See, e.g., United States v. Hewitt, 663 F.2d 1381, 1385 (11th Cir. 1981) (describing elements of aiding and abetting a violation of 18 U.S.C. § 844(h)).

²⁶ Judge Hand's view of the intent required for criminal aiding and abetting was not shared by all courts, some of which argued that it was sufficient that the aider and abettor knew of the purpose of the principal -- i.e., that the crime was a natural consequence of the assistance. The classic statement of this position is found in Backun v. United States, 112 F.2d 635, 636-37 (4th Cir. 1940). The Supreme Court, in Nye & Nissen, nominally resolved the debate by adopting Judge Hand's view. But see United States v. Ortega, 44 F.3d 505, 508 (7th Cir. 1995) (defendant could be culpable of aiding and abetting even in the absence of evidence that he wanted the

unlawful act to succeed, if defendant "rendered assistance that he believed would (whether or not he cared that it would) make the principal's success more likely"); United States v. Zafiro, 945 F.2d 881, 887-88 (7th Cir. 1991) (dicta) (aiding and abetting should be established even absent intent to assist illegal activity, if abettor "knowingly provides essential assistance" that cannot readily be obtained from other sources), *aff'd* on other grounds, 506 U.S. 534 (1993).

²⁷ See, e.g., Superior Growers, 982 F.2d at 177-78; United States v. Campa, 679 F.2d 1006, 1013 (1st Cir. 1982).

²⁸ See United States v. Giovannetti, 919 F.2d 1223, 1227 (7th Cir. 1990) (citing American Law Institute, Model Penal Code § 2.06(3) (a)(ii)). Although attempted aiding and abetting is not a crime, the converse is not true: it is unlawful to aid and abet an attempted crime, provided the underlying attempt is itself an unlawful act.

²⁹ The substantive crimes that may not be "support[ed]" under section 323 are: 18 U.S.C. §§ 32, 37, 81, 175, 351, 831, 842(m) and (n), 844(f) and (i), 956, 1114, 1116, 1203, 1361, 1362, 1363, 1366, 1751, 2155, 2156, 2280, 2281, 2332, 2332a, 2332b, and 2340A, and 49 U.S.C. § 46502.

³⁰ The full definition of "material support or resources" is: "currency or other financial securities, financial services, lodging, training, safehouses, false documentation or identification, communications equipment, facilities, weapons, lethal substances, explosives, personnel, transportation, and other physical assets, except medicine or religious materials." *Id.*

³¹ See H.R. Conf. Rep. No. 482, 103d Cong., 2d Sess. 232 (1994) (noting that, under the original version of 18 U.S.C. § 2339A, it would not be necessary to prove that the facilitator had a "specific intent to commit the underlying action").

³² Accord Model Penal Code § 2.02(2)(b)(ii) (Official Draft and Revised Comments, 1985); *id.*, Explanatory Note on § 2.02, at 236-37 n.13; United States v. Meling, 47 F.3d 1546, 1558 (9th Cir.), *cert. denied*, 116 S. Ct. 130 (1995); United States v. Powell, 929 F.2d 724, 726, 728 (D.C. Cir. 1991). The government need not prove that the defendant had this level of knowledge with respect to all of the particular details of the future result, such as the identity of those who are harmed. Meling, 47 F.3d at 1558. Thus, under section 323, for example, if a defendant was virtually certain that particular recipients would in fact use the provided resources to commit a terrorist crime, it would be immaterial whether the defendant knew precisely when or where the criminal conduct would occur.

³³ Insofar as it can be argued that Congress intended that "training" be considered a "physical asset" for purposes of the statute, a strong argument could be made that a book containing the substance of such "training" also should be considered a "physical asset." But it is unclear whether a court would adopt this reasoning with respect to a book containing information otherwise readily available in the public domain.

³⁴ It is notable that Congress did not prohibit all knowing or intentional facilitation of civil disorders -- it focused principally on such facilitation accomplished by way of teaching or demonstration. Teaching was not Congress's sole focus, however: Subsection 231(a) (2) makes it unlawful to "transport[] or manufacture[] for transportation in commerce any firearm, or explosive or incendiary device, knowing or having reason to know or intending that the same will be used unlawfully in furtherance of a civil disorder." It appears that Congress simply addressed those forms of facilitation -- teaching (§ 231(a)(1)) and the transport of weapons (§ 231(a)(2)) -- that were the most apparent threats to civil order not already addressed adequately by accomplice and conspiracy prohibitions.

³⁵ In addition, the United States Attorney for the District of Arizona recently brought an indictment under § 231(a)(1) against six members of the "Viper" Militia who allegedly had been engaged in, or had conspired to engage in, substantial and detailed training of others in the means by which explosives could be used in civil disorders. United States v. Nelson, et al., Cr-96-280-PHX-EHC (D. Ariz.). In December 1996, all six defendants admitted their guilt. Three defendants pled guilty to a substantive violation of § 231(a)(1), and three others pled guilty to conspiracy to violate § 231(a)(1).

³⁶ Although this is a demanding standard, nonetheless a person teaching the use of explosives cannot avoid culpability by deliberately ignoring facts that would lead him to be aware that the recipient of the teaching is "practically certain" to use it in furtherance of a civil disorder. See generally 1 E. Devitt, C. Blackmar, M. Wolff & K. O'Malley, Federal Jury Practice and Instructions § 17.09 (4th ed. 1992).

³⁷ See, e.g., 141 Cong. Rec. S7685 (daily ed. June 5, 1995) (statement of Sen. Feinstein); 142 Cong. Rec. S7273 (daily ed. June 28, 1996) (statement of Sen. Feinstein). See also 141 Cong. Rec. S7684-85 (daily ed. June 5, 1996) (statement of Sen. Hatch) (agreeing to

inclusion of "intent" requirement in Feinstein Amendment).

³⁸ See, e.g., 141 Cong. Rec. S7685 (daily ed. June 5, 1995) (statement of Sen. Biden) (describing situation where information is sent to a particular person who has expressly indicated that he desires such information so that he can make unlawful use of it); 142 Cong. Rec. S3449 (daily ed. Apr. 17, 1996) (statement of Sen. Biden) (same); 142 Cong. Rec. S7274 (daily ed. June 28, 1996) (statement of Sen. Biden) (same).

³⁹ 141 Cong. Rec. S7683 (daily ed. June 5, 1995) (statement of Sen. Feinstein).

⁴⁰ Id. at S7684-85 (statement of Sen. Hatch); see also id. at S7685 (statement of Sen. Biden) (agreeing with Senator Hatch that explosives manufacturers should not be subject to culpability simply because there is a chance that some persons who receive information from the manufacturers might use that information for unlawful purposes). Senator Hatch apparently was concerned about whether the statute would deter manufacturers from providing lessons on the manufacture and use of explosives. But it should be noted that the Feinstein Amendment would only have restricted the dissemination of information concerning the "making" or "manufacture" of explosive materials, and not the use of such materials.

⁴¹ In addition, Perry followed instructional references from Hit Man in planning and executing the murders, including information about: how to solicit and obtain prospective clients in need of murder-for-hire services; requesting up-front money for expenses; registering at a motel in the vicinity of the crime, paying with cash and using a fake license tag number; committing the murders at the victims' home; how to make the crime scene look like a burglary; cleaning up and carrying away the ejected shells; breaking down the gun and discarding the pieces along the roadside after the murders; and using a rental car with a stolen tag. Id. at 840.

⁴² As explained *infra* note 71, there was some dispute between the parties as to the meaning of this "intent" stipulation, and the court's resolution of that dispute affected its ultimate constitutional analysis.

⁴³ As we explain *infra* at 39 n.62, 43, 44-45 n.71, we think that the district court's First Amendment analysis in *Rice* is, in some respects, open to question. Plaintiffs have appealed the district court decision to the United States Court of Appeals for the Fourth Circuit. Rice v. Paladin Enterprises, Inc., No. 96-2412.

⁴⁴ The Feinstein Amendment was addressed to the dissemination by private persons of bombmaking information that has not been classified. Accordingly, our discussion of the First Amendment is limited to situations in which the government seeks to restrict the dissemination of such privately generated, unclassified information. This Report does not discuss in any detail the constitutionality of governmental restrictions on its own employees' activities to ensure that those employees do not disclose classified information belonging to the government itself. See *supra* note 11. As the Supreme Court explained in Snepp v. United States, 444 U.S. 507, 509 n.3 (1980), such restrictions on employee conduct generally will not violate the First Amendment so long as they are a "reasonable means" of protecting the government's "compelling interest in protecting . . . the secrecy of information important to our national security." See also, e.g., United States v. Morison, 844 F.2d 1057 (4th Cir.), cert. denied, 488 U.S. 908 (1988); McGehee v. Casey, 718 F.2d 1137 (D.C. Cir. 1983).

⁴⁵ See also NAACP v. Claiborne Hardware, Inc., 458 U.S. 886, 927-28 (1982).

⁴⁶ See High Oil' Times, Inc. v. Busbee, 456 F. Supp. 1035, 1040 (N.D. Ga. 1978) (no instance in which the written word alone has ever met the Brandenburg test), aff'd, 621 F.2d 141 (5th Cir. 1980). See also Herceg v. Hustler Magazine, Inc., 814 F.2d 1017, 1023 (5th Cir. 1987) (questioning, but not deciding, whether the Brandenburg test could ever be satisfied by written materials), cert. denied, 485 U.S. 959 (1988). In the early days of the Supreme Court's First Amendment jurisprudence, by contrast, the Court repeatedly held that the Constitution did not protect published, written advocacy of unlawful conduct. See, e.g., Fox v. Washington, 236 U.S. 273 (1915); Schenck v. United States, 249 U.S. 47 (1919); Frohwerk v. United States, 249 U.S. 204 (1919); Abrams v. United States, 250 U.S. 616 (1919); Gitlow v. New York, 268 U.S. 652 (1925). The reasoning of these cases does not in any significant sense survive Brandenburg. See Brandenburg, 395 U.S. at 449 (expressly overruling Whitney v. California, 274 U.S. 357 (1927)).

⁴⁷ The First Amendment would not, however, prohibit the evidentiary use of such advocacy to demonstrate a disseminator's intent in conveying bombmaking information. See Wisconsin v. Mitchell, 508 U.S. 476, 489 (1993). Therefore, insofar as criminal culpability for dissemination of such information depends upon the distributors' intent -- for example, upon whether a disseminator of bombmaking manuals had the conscious purpose of helping others to use the information to engage in unlawful conduct, see *infra* at

40-44 -- the substance of the advocacy in such manuals could be used as material evidence of such intent.

⁴⁸ On occasion, the Court has indicated that this demanding standard applies only to information concerning "a matter of public significance." See, e.g., Florida Star, 491 U.S. at 533 (quoting Smith, 443 U.S. at 103). See also Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc., 472 U.S. 749, 759-61 (1985) (plurality opinion) (speech on matters of "purely private concern" entitled to less First Amendment protection in defamation cases); id. at 764 (Burger, C.J., concurring in pertinent part); id. at 773-74 (White, J., concurring in pertinent part). But see Florida Star, 491 U.S. at 541 (omitting the "matter of public significance" standard in the Court's ultimate holding, quoted in the text above). However, even if speech of "purely private concern" is entitled to a lesser degree of protection, the Court in Florida Star was willing to conclude that the identity of a rape victim is a "matter of public significance." If that is so, it is safe to assume the Court would find that information on how to construct explosives likewise concerns a "matter of public significance."

⁴⁹ In Florida Star, the Court noted that the state's interest in "the physical safety of [rape] victims, who may be targeted for retaliation if their names become known to their assailants," was a "highly significant" interest. 491 U.S. at 537. Presumably, the governmental interest in preventing the havoc caused by explosive-related crimes is at least as, if not more, significant.

⁵⁰ See, e.g., Herceg v. Hustler Magazine, Inc., 814 F.2d 1017 (5th Cir. 1987) (First Amendment bars liability against magazine where reader accidentally committed suicide while attempting technique of autoerotic asphyxiation described therein), cert. denied, 485 U.S. 959 (1988); Yakubowicz v. Paramount Pictures Corp., 536 N.E.2d 1067 (Mass. 1989) (First Amendment bars liability against producer of motion picture where viewers killed a youth while allegedly imitating the violence depicted therein); DeFilippo v. NBC, Inc., 446 A.2d 1036 (R.I. 1982) (First Amendment bars liability against television network where viewer accidentally committed suicide while attempting hanging stunt he saw on the "Tonight Show"); Olivia N. v. NBC, Inc., 126 Cal. App. 3d 488 (Cal. Ct. App. 1981) (First Amendment bars liability against television network where viewers raped a minor with a bottle while allegedly imitating such a rape depicted in television drama). See generally Greenawalt, Speech, Crime, supra note 20, at 284-85 (1989):

Certain artistic depictions and portrayals may lead some members of the audience to commit crimes, and that possibility exists in connection with work that undeniably constitutes expression as well as work whose status is more arguable. Sex and violence, and particularly violent sex, are the main subjects of concern. . . . These asserted connections are plainly an inadequate basis for holding the communicators criminally liable for the crimes that may be committed after exposure to the communication. In any real instance, the most that can be said is that the communicator disregarded a risk that what he said would cause criminal behavior, a risk of which he was aware or should have been aware. Given the extreme difficulty of estimating that in any particular instance the person who receives the communication, or even one of an audience of millions, will commit a crime as a consequence, demonstrating a substantial and unjustifiable risk of the sort needed to establish recklessness or negligence would be very hard. In any event, the First Amendment would preclude liability on those theories because courts and jurors should not be in the business of assessing the unjustifiability of risks by engaging in ad hoc weighing of the expressive value of a particular program or communication against the dangers it creates. . . . The dangers of interference with forms of expression are grave enough also to bar civil recovery when victims of crimes by consumers sue those responsible for communications on a theory of reckless or negligent causation. For example, if a viewer "acts out" a violent scene from a television drama, the victim cannot recover against the company that has shown the program. . . . If portrayals in literature, movies, television, photography, and the fine arts may ever be forbidden or made the subject of civil liability because of a propensity to

cause crimes, the great danger of a particular sort of communication must be powerfully shown, and the proscribed communications must be very clearly defined.

⁵¹ See, e.g., Smith v. Linn, 563 A.2d 123 (Pa. Super. Ct. 1989) (First Amendment barred liability against publisher of diet book after reader died as result of following diet), aff'd mem., 587 A.2d 309 (Pa. 1991); Alm v. Van Nostrand Reinhold Co., 480 N.E.2d 1263 (Ill. App. Ct. 1985) (First Amendment barred liability against publisher of "how-to" book where reader had been injured while following instructions therein); Walt Disney Productions, Inc. v. Shannon, 276 S.E.2d 580 (Ga. 1981) (First Amendment barred liability against producer and broadcaster of television program where child sustained injuries while seeking to reproduce a sound effect demonstrated for children on "Mickey Mouse Club"). Cf. Winter v. G.P. Putnam's Sons, 938 F.2d 1033 (9th Cir. 1991) ("[g]uided by the First Amendment and the values embodied therein," id. at 1036, court held that mere negligence could not form the basis of liability against book publisher where mushroom enthusiasts became ill from eating mushrooms that the book had described as safe to eat).

⁵² See, e.g., American Booksellers Ass'n v. Hudnut, 771 F.2d 323, 328-29 (7th Cir. 1985) (statute permitting civil liability against producers of depictions of sexually explicit subordination of women is unconstitutional, even accepting the premises that "[m]en who see women depicted as subordinate are more likely to treat them so" and that people are likely to "act in accordance with the images and patterns" they find in such expression), aff'd mem., 475 U.S. 1001 (1986); Video Software Dealers Ass'n v. Webster, 968 F.2d 684 (8th Cir. 1992) (invalidating on constitutional grounds state statute prohibiting the sale or rental to minors of videos "depicting violence"); Eclipse Enterprises v. Gulotta, 942 F. Supp. 801 (E.D.N.Y. 1996) (invalidating on constitutional grounds local law criminalizing sale to minors of trading cards depicting a "heinous crime, an element of a heinous crime, or a heinous criminal"); Zamora v. CBS, 480 F. Supp. 199 (S.D. Fla. 1979) (First Amendment bars liability against television networks to recover damages where television violence allegedly caused viewer to become addicted and desensitized to violent behavior, resulting in his killing an 83-year-old woman). See also Watters v. TSR, Inc., 715 F. Supp. 819 (W.D. Ky. 1989) (First Amendment bars liability against manufacturer of "Dungeons and Dragons" game for failure to warn, where "mentally fragile" person committed suicide after having become consumed with the role-playing nature and fantasy of the game), aff'd on other grounds, 904 F.2d 378 (6th Cir. 1990). Cf. Winters v. New York, 333 U.S. 507, 519 (1948) (invalidating as unconstitutionally vague a criminal law that had been construed to prohibit circulation of publications depicting violence that "influence generally persons to commit crimes of violence against the person").

The results of the First Amendment analysis do not change if these cases are alternatively viewed as involving implied advocacy of undesirable or unlawful conduct. For example, in Kingsley Int'l Pictures Corp. v. Regents of the Univ. of New York, 360 U.S. 684 (1959), the State refused to grant a license for exhibition of the film "Lady Chatterley's Lover," because that film allegedly "present[s] . . . adultery as a desirable, acceptable and proper pattern of behavior." Id. at 685. The Court characterized the State as having "prevent[ed] the exhibition of a motion picture because that picture advocates an idea -- that adultery under certain circumstances may be proper behavior." Id. at 688. Even ten years prior to Brandenburg, the Court held that the Constitution "protects advocacy of the opinion that adultery may sometimes be proper, no less than advocacy of socialism or the single tax." Id. at 689.

⁵³ 491 U.S. at 541. For example, although Florida Star strongly suggests that the government cannot impose "categorical prohibitions," id. at 539, on the dissemination of a prescribed type of information -- without regard to scienter, the reasonableness of the disclosure, the efficacy of the restriction, and the manner in which the State otherwise can prevent the information's disclosure -- the Court nevertheless implied in Florida Star that the First Amendment might permit liability under the common law tort of invasion of privacy for dissemination of true, lawfully obtained information, where the government has not facilitated the disclosure of the information, the information had not previously been publicized, a reasonable person would find the disclosure of the information "highly offensive," and some scienter requirement is satisfied. Id. at 538-40.

⁵⁴ See also Oklahoma Pub. Co. v. District Court, 430 U.S. 308, 311-12 (1977) (per curiam); Nebraska Press Ass'n v. Stuart, 427 U.S. 539, 595-96 (1976) (Brennan, J., concurring):

Much of the information that the Nebraska courts enjoined petitioners from publishing was already in the public domain, having been revealed in open court proceedings or through public documents. Our prior cases have foreclosed any serious contention that further disclosure of such information can be suppressed before publication or even punished after publication.

An infamous case in which this principle was put to the test involved the prior restraint imposed upon publication by the periodical

the Progressive of an article describing technical processes of thermonuclear weapons. See United States v. Progressive, Inc., 467 F. Supp. 990 (W.D. Wis.), rehearing denied, 486 F. Supp. 5 (W.D. Wis.), appeal dismissed, 610 F.2d 819 (7th Cir. 1979). While there is, to this day, substantial debate about whether the prior restraint violated the First Amendment, the district judge in that case acknowledged that such a restraint could be imposed, if at all, only because significant and dangerous information in the article was not "in the public realm." 467 F. Supp. at 993, 999. "[N]owhere in the public domain is there a correct description of the type of design used in United States thermonuclear weapons." Id. at 999. (The information at issue in that case had been classified as "Restricted Data," id. at 998, although the author of the article had not had access to any classified documents. See supra note 12 (discussing "Restricted Data" under the Atomic Energy Act).) The magazine moved for rehearing on the ground that the information was in fact in the public domain; but the district court once more found that the article "contains a comprehensive description of radiation coupling, along with [two] other . . . key concepts, that is not found in the public realm." 486 F. Supp. at 9. The plain import of the district court's decisions is that the prior restraint could not be imposed if the critical information were, in fact, "in the public realm." The government seemed to concede this point: During pendency of the Progressive's appeal of the prior restraint, the substance of the article was published in other journals, see L.A. Powe, Jr., The H-Bomb Injunction, 61 U. Colo. L. Rev. 55, 70 (1990), at which time the government moved for dismissal of the appeal, see 610 F.2d 819. Thereafter, the Progressive published the article, and the government never attempted to prosecute anyone for publication of the information after such information was in the public domain.

⁵⁵ Brandenburg, 395 U.S. at 456 (Douglas, J., concurring).

⁵⁶ A related principle is that generally applicable common-law causes of action typically will not offend the First Amendment in cases where they are applied to expressive conduct such as publication or broadcast. See, e.g., Cohen v. Cowles Media Co., 501 U.S. 663 (1991) (First Amendment does not bar liability for breach of contract where defendant newspaper published confidential source's name); Zacchini v. Scripps-Howard Broadcasting Co., 433 U.S. 562 (1977) (First Amendment does not bar liability for tort of unlawful appropriation of "right to publicity" where television station broadcast "human cannonball" act in its entirety). However, it should be noted that the First Amendment does impose significant limits on the use of a "generally applicable" cause of action where an element of that cause of action inevitably (or almost always) depends on the communicative impact of speech or expression. See, e.g., Hustler Magazine, Inc. v. Falwell, 485 U.S. 46 (1988) (First Amendment generally does not permit liability, under the generally applicable tort of intentional infliction of emotional distress, for publication of a parody of a public figure). See also Cohen, 501 U.S. at 671 (distinguishing Hustler).

⁵⁷ See generally Greenawalt, Speech, Crime, supra note 20.

⁵⁸ Accord United States v. Mendelsohn, 896 F.2d 1183, 1186 (9th Cir. 1990) ("No first amendment defense need be permitted when words are more than mere advocacy, `so close in time and purpose to a substantive evil as to become part of the crime itself.'") (citation omitted); United States v. Barnett, 667 F.2d 835, 842 (9th Cir. 1982) ("The first amendment does not provide a defense to a criminal charge simply because the actor uses words to carry out his illegal purpose. Crimes . . . frequently involve the use of speech as part of the criminal transaction."). This rationale applies, for instance, to conspiracies and other unlawful agreements. See Brown v. Hartlage, 456 U.S. 45, 55 (1982): "The fact that . . . an [unlawful] agreement necessarily takes the form of words does not confer upon it, or upon the underlying conduct, the constitutional immunities that the First Amendment extends to speech." See also United States v. Rowlee, 899 F.2d 1275, 1278 (2d Cir.) (First Amendment does not protect speech acts constituting an illegal conspiracy), cert. denied, 498 U.S. 828 (1990); United States v. Fleschner, 98 F.3d 155, 158-59 (4th Cir. 1996) (First Amendment does not protect speech acts in furtherance of an illegal conspiracy).

⁵⁹ Accord Barnett, 667 F.2d at 842-43; United States v. Buttorff, 572 F.2d 619, 623-24 (8th Cir.), cert. denied, 437 U.S. 906 (1978).

⁶⁰ See Greenawalt, Speech, Crime, supra note 20, at 85:

Much more commonly than people commit noncommunicative crimes "purely" by communication, they cooperate, by talking, in the commission of crimes that involve noncommunicative acts. . . . The reasons of ordinary penal policy for covering communicative efforts to carry out ordinary crimes are obvious, and the criminal law sensibly draws no distinction between communicative and other acts.

Although assertions of fact generally fall within a principle of freedom of speech, what these sorts of factual statements

contribute to

the general understanding of listeners is minimal, and the justifications from free speech that apply to speakers do not reach communications that are simply means to get a crime successfully committed. The relevance of free speech is so slight in

respect

to such highly specific information related to an immediate practical purpose that it can be disregarded here.

⁶¹ For cases recognizing this distinction, see, e.g., United States v. Johnson, 952 F.2d 565, 578 n.13 (1st Cir. 1991), cert. denied, 506 U.S. 816 (1992); Rowlee, 899 F.2d at 1279-80; Freeman, 761 F.2d at 552; Buttorff, 572 F.2d at 624 (defendants went "beyond mere advocacy": they "explained how to avoid withholding"); People v. Bohmer, 120 Cal. Rptr. 136, 144 n.1 (Cal. Ct. App.), cert. denied, 423 U.S. 990 (1975). See also Greenawalt, Speech, Crime, supra note 20, at 247 n.13. In Freeman, for example, Justice (then Judge) Kennedy concluded that, because some of the counts of the indictment arguably were premised on the defendant's abstract advocacy of tax evasion, a Brandenburg-like jury instruction was appropriate for such counts. Id. at 551-52. But where the defendant directly counseled someone on how to file false tax returns, "a First Amendment defense is foreclosed even if the prosecution rests on words alone." Id. at 552. Conversely, advocacy of unlawful conduct is entitled to the protection of the Brandenburg test, which cannot be circumvented merely by labeling such advocacy as "aiding and abetting." See, e.g., Gay Lesbian Bisexual Alliance v. Sessions, 917 F. Supp. 1548, 1556 (M.D. Ala. 1996). See also Bond v. Floyd, 385 U.S. 116, 133 (1966). In this regard, it is worth noting that the general federal aiding and abetting statute -- 18 U.S.C. § 2 -- punishes as a principal whoever "counsels" a federal offense. See supra note 22. We are not aware of any modern case in which culpability under § 2 was premised solely on "counseling" in the form of encouragement (or advocating that a crime be committed), without any actual aid or assistance to the principal. Insofar as § 2 were construed to permit culpability in such a "pure" advocacy situation, it is likely -- at least absent special circumstances, such as implicit coercion or a fiduciary relationship between the pertinent parties -- that the prosecution would be required to satisfy the Brandenburg standards. See also supra note 20.

⁶² The district court in Rice v. Paladin, see supra at 27-28, thus erred in concluding that the Brandenburg standard applies to speech "which advocates or teaches lawless activity." 940 F. Supp. at 845 (emphasis added). As we explain in the text, the constitutional analysis can differ quite a bit depending on whether a case involves the "advocacy" or the "teaching" of lawless activity.

⁶³ As Professor Emerson suggests, there may not always be a bright line between "advising" a group of persons that they should engage in criminal conduct and "teaching" that same group specific techniques that the teacher intends for the group to use in such crimes: in particular factual circumstances, these are likely to be two points on a fluid continuum of conduct. Whether a particular instance of teaching will fall outside the Brandenburg protections for advocacy likely will depend on the "explicitness and concreteness" of the teaching. Scales, 367 U.S. at 253. Teaching "in the abstract" the philosophical or political beliefs of a certain author is constitutionally protected, see id. at 252 n.27; while, on the other end of the scale, instruction on how to use a pencil to kill a person in the case of an uprising, see id. at 250-51, is not protected (at least insofar as the teacher intends for the students to make use of such a technique). Somewhere in the middle are cases having aspects both of advocacy and of "teaching." For instance, exhorting a crowd of young men to "avoid the draft by feigning insanity (or burning your draft cards)" in some sense "teaches" the audience a method of unlawful conduct; but it does not really provide the audience any information it does not already know, and thus probably should more appropriately be viewed as a form of advocacy entitled to some constitutional solicitude (albeit not as much as that to which "pure" advocacy is entitled).

⁶⁴ See also Gorin v. United States, 312 U.S. 19, 27-28 (1941) (in order to avoid a serious constitutional question, Court construes "intent" requirement in espionage statute dealing with dissemination of information to "require[] those prosecuted to have acted in bad faith") (emphasis added).

⁶⁵ Perhaps the First Amendment would impose a requirement that there be some realistic risk that the crime will occur. For example, if the information is conveyed to persons who would not under any circumstances use it for unlawful ends, the threat of danger is so remote that the speech arguably should not be punished regardless of bad intent. Courts might find, for example, that culpability can attach only where the defendant both intended and had reason to believe that the information would or could be unlawfully used. Cf. United States v. Dworkin, 855 F.2d 12, 19 & n.6 (1st Cir. 1988).

⁶⁶ It is important once again to distinguish training with bad intent from advocacy with bad intent. Though a purpose to facilitate a crime is sufficient to permit punishment of the former, such a bad purpose is necessary but not sufficient when it comes to restrictions on pure advocacy; in the latter case, Brandenburg imposes the additional requirements (i) that the speech be directed to inciting imminent crime, and (ii) that such imminent wrongdoing is likely to occur, in fact.

⁶⁷ For example, the cases where a private party has sought to impose tort liability on the basis of "negligent" or "reckless" publication or broadcast, see supra at 31-33 & notes 50-53, have not involved situations where the publisher or broadcaster had the purpose of fomenting criminal conduct. Such intent is present in aiding-and-abetting and conspiracy cases, but in those cases, the person providing the information is, in a much more direct sense, actually participating with the recipient of the information in the performance of an illegal act.

The precedents that come closest to the situation described in the text are the aiding-and-abetting decisions in Buttorff and Barnett. See supra note 24. In Buttorff, the court of appeals rejected a First Amendment argument where the "joint participation" consisted of tax-evasion instructions that defendants provided at "large public gatherings," presumably to persons they did not personally meet. 572 F.2d at 622-23. In Barnett, a First Amendment argument was rejected (albeit in the context of determining whether there was probable cause for a warrant to search premises) where the only contact between the accomplice and the principal was that the latter received from the former mail-order instructions for the manufacture of phencyclidine, along with the name of a "reliable" chemical supplier, in exchange for the \$10 purchase price. 667 F.2d at 840. As explained in note 24, supra, there is some question whether aiding and abetting can be established by virtue of arms-length transactions such as those in Buttorff and (especially) Barnett. But that is quite a different question than whether the Constitution would bar such culpability. Insofar as those cases hold that there is no First Amendment defense for transmission of information with the intent to facilitate crimes, they are consistent with the conclusion we reach in the text above.

⁶⁸ The recent case of United States v. Aguilar, 115 S. Ct. 2357 (1995), provides further support for permitting prohibition of improperly motivated publication of dangerous instructional information. The defendant in that case urged a narrow construction of a statute banning disclosure of wiretap authorizations, on the ground that a broad reading of the statute would threaten to violate the principle that "the government may not generally restrict individuals from disclosing information that lawfully comes into their hands in the absence of a 'state interest of the highest order.'" Id. at 2365 (quoting Smith, 443 U.S. at 103). The Court, while endorsing that basic principle, nonetheless rejected defendants' argument, in part on the ground that "the statute here in question does not impose such a restriction generally, but only upon those who disclose wiretap information 'in order to [ob]struct, impede, or prevent' a wiretap interception. Id. (quoting 18 U.S.C. § 2232(c)).

There are many other contexts, as well, in which First Amendment protection depends upon whether a speaker has some "bad" intent, rather than on the degree of harm that the speech might cause. For example, advocacy of unlawful action will be treated very differently under Brandenburg depending on whether it is "directed to" inciting imminent unlawful conduct, even though such a bad intent does not ordinarily increase the threat to public safety. Similarly, under the earlier Smith Act cases, the Court, in order to avoid serious constitutional questions, strained to construe the Act to require bad intent, even though such intent should not have been relevant if, as the Court insisted, the touchstone for constitutional analysis was the risk of a "clear and present danger." See, e.g., Scales, 367 U.S. at 221-22, 229-30; Dennis, 341 U.S. at 499-500 (plurality opinion). See also id. at 516 (defendants' intent and their "power to bring about the evil" were separate necessary elements of the offense). And, most famously, the First Amendment prohibits imposition of liability for publication of a false and defamatory statement about a public figure, unless the publisher acts with "actual malice," i.e., with knowledge that the statement was false or with reckless disregard of whether it was false or not. See, e.g., Masson v. New Yorker Magazine, Inc., 501 U.S. 496, 510 (1991); New York Times Co. v. Sullivan, 376 U.S. 254, 279-80 (1964). Similarly, the Court in Florida Star suggested that, whereas the categorical prohibition on the publication of rape victims' names at issue in that case was unconstitutional, the constitutional calculus might be different if the statute included a scienter requirement. 491 U.S. at 539.

⁶⁹ See Greenawalt, Speech, Crime, supra note 20, at 273: "The constitutional standard here should be that a person intend that the crime be committed and that it be reasonably likely that it will be committed in the 'near future.'" See also supra note 65.

⁷⁰ See 141 Cong. Rec. S7683 (daily ed. June 5, 1995) (statement of Sen. Feinstein) (describing instructions from the Terrorist Handbook for construction of items -- such as "toilet paper roll booby traps" and "baby food bombs" --- the sole purpose for which allegedly is "to kill somebody"). Cf. Posters 'n' Things, Ltd. v. United States, 511 U.S. 513, 521 & n.11 (1994) (construing statutory prohibition on sale of items "primarily intende. . . for use" with drugs to cover "multiple-use" items for which the "likely use" by "customers generally" is drug-related).

⁷¹ In a civil case, on the other hand, Professor Greenawalt's concern about constraining juries' discretion would be more directly implicated, but the First Amendment should be no bar where an improper intent is proved by clear and convincing evidence. See, e.g., Masson, 501 U.S. at 510; Gertz v. Robert Welch, Inc., 418 U.S. 323, 342 (1974). In Rice v. Paladin itself, the publishers of Hit Man had no specific knowledge that they had sold the book to particular persons who planned to commit a crime. Therefore, for reasons

discussed in this Report, the First Amendment would permit liability to attach only if defendants had the requisite "intent" that Hit Man be used to facilitate crimes. For purposes of summary judgment, defendants stipulated that they "intended" that "their publications would be used, upon receipt, by criminals and would-be criminals to plan and execute the crime of murder for hire, in the manner set forth in the publications." Joint Statement of Facts ¶ 4b (referenced at 940 F. Supp. at 840). That concession would, for purposes of summary judgment, seem to foreclose a constitutional defense, except for the fact that defendants argued (in their briefs) that all they meant by this stipulation of "intent" was that they "knew" the information contained in Hit Man would be read and used by an audience that includes criminals. See Memorandum of Points and Authorities in Support of Defendant Paladin Enterprises, Inc.'s Motion for Summary Judgment, at 14; Reply Memorandum of Points and Authorities in Support of Defendant Paladin Enterprises, Inc.'s Motion for Summary Judgment, at 14-15. In other words, defendants argued that they had stipulated to "intent" only in the sense that that concept is understood in the civil tort context: *i.e.*, one "intends" the natural consequences of one's acts. Accordingly, defendants argued, they only "intended" that Hit Man would be used for unlawful purposes in the same way that Stephen King "intends" his novels will be used for unlawful purposes: in both cases, the publisher allegedly "knows" that publication likely will "produce" unlawful conduct by some, unknown, reader or readers. Reply Memorandum of Points and Authorities in Support of Defendant Paladin Enterprises, Inc.'s Motion for Summary Judgment, at 15. As we have explained in this memorandum, the First Amendment does not permit a publisher of factual information to be subject to liability merely on the basis of this type of "intent." See *supra* at 30-34. Invoking this principle, the district court in *Rice* granted Paladin's motion for summary judgment, but only because the court accepted Paladin's representation that the stipulation of "intent" meant only that Paladin "knew" that some readers would misuse the book's information. 940 F. Supp. at 846.

However, even assuming *arguendo* that the defendants' own construction of the "intent" stipulation were correct, that still would not justify the grant of summary judgment, since it would leave unanswered the question whether Paladin also had the specific purpose of facilitating murder. Paladin stipulated (for purposes of summary judgment) that it engaged in a marketing strategy intended to maximize sales to the public, including to "criminals and would-be criminals who desire information and instructions on how to commit crimes." As we explain in the text, if Paladin in effect encourages unlawful use of its product so that it can increase its profits - for instance, if Hit Man is "offered for sale in such a mode as purposely to attract purchasers who want[] [it] for the unlawful [use]," *Danovitz*, 281 U.S. at 397 -- or if there is other evidence that Paladin publishes Hit Man with the actual purpose of furthering criminal conduct, the publisher might be found to have sold Hit Man for the purpose of facilitating murder. If the finder of fact determined that that "intent" was proved by clear and convincing evidence, the First Amendment should not bar liability. We also should note, however, that, wholly apart from the First Amendment question, it is not clear whether the plaintiffs in *Rice* alleged a cognizable "aiding and abetting" tort claim under Maryland law, a question that we have no occasion to address. *But see supra* note 24 (discussing whether, under federal criminal law, aiding and abetting can be established by virtue of arms-length transactions with anonymous purchasers).

⁷² See also Ariz. Rev. Stat. Ann. § 13-1004 (1996); Ky. Rev. Stat. Ann. § 506.080 (Baldwin 1996); N.D. Cent. Code § 12.1-06-02 (1995).

⁷³ As far as we can tell, there are no published opinions concerning the use of such statutes to prosecute facilitation committed by way of conveying information, nor have such statutes ever been the subject of a First Amendment challenge.

⁷⁴ Similar prohibitions using a "reasonable cause to believe that the product will be unlawfully used" standard are found in statutes dealing with chemicals and equipment that can be used to produce controlled substances. See, e.g., 21 U.S.C. §§ 841(d)(2) (distribution of chemicals), 843(a)(7) (distribution and export of chemicals, equipment, and other products), 960(d)(3),(4) (export of chemicals).

⁷⁵ See *supra* note 50 (quoting Greenawalt, *Speech, Crime*, *supra* note 20, at 284-85).

⁷⁶ See also, e.g., *United States v. Hayden*, 64 F.3d 126, 133 (3d Cir. 1995) (citing *United States v. Caminos*, 770 F.2d 361, 365-66 (3d Cir. 1985)); *United States v. Honeycutt*, 8 F.3d 785, 787 (11th Cir. 1993), *cert. denied*, 511 U.S. 1024 (1994); *United States v. Feroz*, 848 F.2d 359, 360 (2d Cir. 1988); *United States v. Corral-Martinez*, 592 F.2d 263, 269-70 (5th Cir. 1979). This standard is derived from § 2.02(7) of the Model Penal Code:

When knowledge of the existence of a particular fact is an element of an offense, such knowledge is established if a person is aware of a high probability of its existence, unless he actually believes that it does not exist.

The Ninth Circuit recently held that the § 2.02(7) "aware of a high probability" standard is appropriate "only in situations where the evidence justifies an argument of willful blindness," and that absent a willful blindness situation the government must prove that the defendant had "actual knowledge or awareness" of the existence of the fact constituting an element of an offense. United States v. Aguilar, 80 F.3d 329, 332 (9th Cir. 1996) (en banc). We take issue with this holding. The Model Penal Code definition of "knowledge" conforms to the common understanding of knowledge, and that definition should be used regardless of whether a case involves an issue of "willful blindness." See Jonathan L. Marcus, Note, Model Penal Code Section 2.02(7) and Willful Blindness, 102 Yale L.J. 2231 (1993). To require that a criminal defendant achieve certainty before he can be said to "know" an operative fact would preclude conviction in virtually any case in which a defendant has committed an offense in reliance on information supplied by others. But most of what we "know" as historical fact has been related to us orally or in writing. Indeed, as Justice (then Judge) Kennedy explained in a case involving a related question:

[W]e commonly act on less than complete information and in this world may never know one-hundred-percent certainty. "Absolute knowledge can be had of very few things," said the Massachusetts court, and the philosopher might add "if any." For most practical purposes, "knowledge" is not confined to what we have personally observed or to what we have evolved by our own cognitive faculties."

United States v. Jewell, 532 F.2d 697, 706 n.6 (Kennedy, J., dissenting) (9th Cir.) (quoting Rollin M. Perkins, Criminal Law 775 (2d ed. 1969) (internal citations omitted)), cert. denied, 426 U.S. 951 (1976).

⁷⁷ See, e.g., Leary, 395 U.S. at 47 (defendant's "knowledge" that marijuana was imported can be established if supplier told defendant the source of the drugs).

⁷⁸ For example, persons who, with no bad intent, post information to certain Usenet newsgroups on the Internet may have reason to know that a certain subscriber to that service often expresses intense hatred of the government. While it is uncertain whether a fact-finder would conclude that such knowledge constitutes "reasonable cause to believe that [that subscriber] will use such information for, or in furtherance of," a crime, the chill caused by the risk of such a finding would raise significant First Amendment questions, because, unless there were a way to prevent access to the suspicious person, the content-provider might have little choice but to cease her "postings" altogether. Similarly, a person demonstrating the proper use of explosives to a classroom full of well-intentioned students (or purchasers of the product) may sense that a particular student seems suspicious, or may discover that one listener asks questions that might subtly suggest an improper motive for wanting to learn the techniques in question. The possible application of a facilitation prohibition to such a case might well cause the teacher to cease instruction (or, at the very least, exclude the suspicious-looking persons, where that is feasible). Because of this possibility, courts might be more inclined to question the constitutionality of the prohibition.

⁷⁹ Moreover, as Professor Greenawalt argues, it is unlikely that the First Amendment would permit criminal culpability to attach on a "facilitation" theory absent the speaker's knowledge of a substantial risk that the communication will facilitate a crime:

My own sense is that a legislature may appropriately accept whatever curtailment of expression is involved in a prohibition on facilitation that the actor believes is likely However, a principle of free speech provides a powerful reason why liability should not extend to all negligent or reckless acts of communication, that is, to situations where the speaker is wholly unaware of the use to be made of what he says or thinks there is only some modest risk it will be used for a criminal purpose.

Greenawalt, Speech, Crime, supra note 20, at 87.

⁸⁰ In order to be sustained under the First Amendment, the "intent" scienter requirement in this prohibition must be understood to refer to cases where the person disseminating the information has a "conscious purpose" that it be used unlawfully, or (at the very least) a material stake in seeing that it be used for such purposes. "Intent" should not be construed to encompass cases where criminal activity is not in fact the intended result, but is merely a "foreseeable" result, or a "natural consequence," of the publication of the information in question. Seesupra at 30-34, 40.

⁸¹ In order to avoid a chilling effect on protected speech, courts might construe such a prohibition as limited to cases where it is reasonably likely that the information will in fact facilitate such criminal conduct. See supra at 43 & note 69.

Return to . . . [CCIPS home page](#) || [Justice Department home page](#)

Updated page March 22, 1999
usdoj-crm/mis/mdf

EXHIBIT 11

Chapter I—Department of State**§ 125.01**

tions List equipment in a foreign country without prior Department of State approval provided:

(a) The arrangement calls for delivery of equipment only for use of the person in the United States or an agency of the U.S. Department of Defense;

(b) The technical data of U.S. origin to be used in the foreign manufacture is unclassified, and has been licensed for export by the Department of State or is subject to one of the exemptions in §§ 125.10, 125.11, or 125.12 of this subchapter;

(c) The foreign manufacture is pursuant to a contract or purchase order between a person in the United States and a foreign person for delivery of equipment only to the person in the United States or to an agency of the U.S. Government anywhere in the world;

(d) The contract or purchase order between a person in the United States and a foreign person:

(1) Limits the use of the technical data to that required by the contract or purchase order;

(2) Prohibits the disclosure of the data to any other person except duly qualified subcontractors for the equipment within the same country;

(3) Prohibits the acquisition of any rights in the data by any foreign person without the approval of the Department of State; and

(4) Provides that any subcontracts between foreign persons in the approved country for manufacture of equipment for delivery pursuant to the contract or purchase order contain all the limitations of this paragraph (d); and

(e) The person in the United States provides the Office of Munitions Control, Department of State, with a copy of each subcontract (or Purchase Order) for offshore procurement at the time it is accepted by both persons. Each such subcontract or purchase order must clearly identify the article to be produced.

[Dept. Reg. 108.646, 36 FR 20941, Nov. 2, 1971]

PART 125—UNCLASSIFIED TECHNICAL DATA AND CLASSIFIED INFORMATION (DATA AND EQUIPMENT)

Sec.

125.01 Technical Data.

125.02 Classified information.

125.03 Export of technical data.

125.04 Export of unclassified technical data.

125.05 Export of classified information (data and equipment).

EXEMPTIONS

125.10 Shipments by U.S. Government agencies.

125.11 General exemptions.

125.12 Canadian shipments.

125.13 Data on nuclear materials.

PROCEDURES

125.20 Export of unclassified technical data.

125.21 Export of classified information (data and equipment).

125.22 Certification requirements.

125.23 Filing of licenses for export of unclassified technical data.

125.24 Filing of licenses for export of classified information (data and equipment).

AUTHORITY: Sec. 414, as amended, 68 Stat. 848; 22 U.S.C. 1934; secs. 101 and 105, E.O. 10973, 26 FR 10409; sec. 6, Departmental Delegation of Authority No. 104, 26 FR 10608, as amended, 27 FR 9925, 28 FR 7231; and Redlegation of Authority No. 104-3-A, 28 FR 7231.

SOURCE: Dept. Reg. 108.605, 34 FR 12037, July 17, 1969, unless otherwise noted.

NOTE: Export licenses for technical data may be denied, revoked, suspended, or amended by the Department of State. (See § 123.05 of this subchapter.)

§ 125.01 Technical data.

As used in this subchapter the term "technical data" means: (a) Any unclassified information that can be used, or be adapted for use, in the design, production, manufacture, repair, overhaul, processing, engineering, development, operation, maintenance, or reconstruction of arms, ammunition, and implements of war on the U.S. Munitions List; or (b) any technology which advances the state-of-the-art or establishes a new art in an area of significant military applica-

§ 125.02

bility in the United States;¹ or (c) classified information as defined in § 125.02.

[Dept. Reg. 108.629, 35 FR 19016, Dec. 16, 1970]

§ 125.02 Classified information.

As used in this subchapter, the term "classified information" is either (a) equipment, or (b) information (relating to any arms, ammunition, and implements of war on the U.S. Munitions List) which has been assigned a U.S. security classification as requiring protection in the interest of national defense. (Patent applications covered by a secrecy order fall in the same category as classified information. See § 125.05 (d).) See §§ 125.10 and 125.11 for exemptions.

§ 125.03 Export of technical data.

The export controls of this subchapter over technical data (a) apply to the export of unclassified technical data relating to arms, ammunition, and implements of war on the U.S. Munitions List, and (b) classified equipment and classified information relating to arms, ammunition, and implements of war on the U.S. Munitions List as defined in § 125.02. These controls shall apply whenever the information is to be exported by oral, visual, or documentary means. Therefore, an export occurs whenever technical data is *inter alia*, mailed or shipped outside the United States, carried by hand outside the United States, disclosed through visits abroad by American citizens (including participation in briefings and symposia), and disclosed to foreign nationals² in the United States (including plant

¹The initial burden of determining whether the technology in question advances the state-of-the-art or establishes a new art is upon the U.S. party or applicant in consultation with the cognizant agency of the U.S. armed forces.

²The term "foreign nationals" as used in this subchapter means "All persons not citizens of, not nationals of, nor immigrant aliens to, the United States" as defined in the Department of Defense Industrial Security Manual. However, certain other foreign persons may be cleared to have access to technical data. See section 3 of the Industrial Security Manual.

Title 22—Foreign Relations

visits and participation in briefings and symposia). A license to export technical data shall not be used for foreign production purposes, or for technical assistance in such production, without the specific approval of the Department of State.

§ 125.04 Export of unclassified technical data.

(a) *General.* A license issued by the Department of State shall be required for the export of unclassified technical data (as defined in § 125.01 (a) and (b)) unless otherwise expressly exempted in this subchapter (see §§ 125.10 and 125.11).

Unclassified information that does not meet the definition of technical data or can meet the test of an exemption in §§ 125.10 and 125.11 (see especially § 125.11(a)(2)) shall not be the subject of license applications.

(b) *Patents.* A license issued by the Department of State shall be required for the export of unclassified technical data relating to arms, ammunition, and implements of war which exceed the data used to support a domestic or foreign filing of a patent application. The export of technical data supporting the filing and prosecution of patent applications in foreign countries is subject to regulations issued by the U.S. Patent Office under 35 U.S.C. 184.

(c) *Visits.* A license issued by the Department of State shall be required for the export of unclassified technical data relating to arms, ammunition, and implements of war on the U.S. Munitions List which are to be disclosed to foreign nationals either in connection with visits to foreign countries, including foreign diplomatic missions and consular offices in the United States and abroad, by U.S. persons, or in connection with visits to the United States by foreign nationals, unless otherwise expressly exempted in this subchapter (see § 125.11).

[Dept. Reg. 108.605, 34 FR 12037, July 17, 1969, as amended at Dept. Reg. 108.615, 35 FR 3030, Feb. 14, 1970; Dept. Reg. 108.629, 35 FR 19016, Dec. 16, 1970]

Chapter I—Department of State**§ 125.11****§ 125.05 Export of classified information (data and equipment).**

(a) Any request for authority to export classified information (data or equipment) by other than the cognizant department or agency of the U.S. Government shall be submitted to the Department of State for approval. (See §§ 125.10 and 125.11 for exemptions.) The application shall set forth all pertinent information with full details of the proposed transaction. (See § 125.21 for procedure.)

(b) Classified information, as defined in § 125.02, which is approved by the Department of State for export shall be transferred or communicated only in accordance with the requirements of the Department of Defense Industrial Security Manual relating to the transmission of classified information (and any other requirements imposed by cognizant U.S. departments and agencies).

(c) The approval of the Department of State shall be obtained for the export of classified information to be disclosed to foreign nationals either in connection with visits to foreign countries by U.S. persons, or in connection with visits to the United States by foreign nationals, unless the proposed export is expressly exempt under the provisions of this subchapter (see § 125.11). There shall be no release of classified information in any manner or form to any foreign national except as otherwise expressly provided in this subchapter.

(d) All communications relating to a patent application covered by a secrecy order shall be addressed to the U.S. Patent Office. (See 37 CFR 5.11.)

[Dept. Reg. 108.605, 35 FR 12037, July 17, 1969, as amended by Dept. Reg. 108.615, 35 FR 3030, Feb. 14, 1970]

EXEMPTIONS**§ 125.10 Shipments by U.S. Government agencies.**

Exports of technical data by U.S. Government agencies are exempt in accordance with Part 126 of this subchapter. This exemption, however, shall not apply when a U.S. Government agency, on behalf of a private individual or firm, acts as a transmittal

agent either as a convenience or in satisfaction of security requirements.

§ 125.11 General exemptions.

(a) Except as provided in § 126.01, district directors of customs and postal authorities are authorized to permit the export without a license of unclassified technical data as follows:

(1) If it is in published³ form and subject to public dissemination by being:

(i) Sold at newstands and bookstores;

(ii) Available by subscription or purchase without restrictions to any person or available without cost to any person;

(iii) Granted second class mailing privileges by the U.S. Government; or,

(iv) Freely available at public libraries.

(2) If it has been approved for public release by any U.S. Government department or agency having authority to classify information or material under Executive Order 11652, as amended, and other applicable Executive Orders, and does not disclose the details of design, production, or manufacture of any arms, ammunition, or implements of war on the U.S. Munitions List.

(3) If the export is in furtherance of a manufacturing license or technical assistance agreement approved by the Department of State in accordance with Part 124 of this subchapter.

(4) If the export is in furtherance of a contract with an agency of the U.S. Government or a contract between an agency of the U.S. Government and foreign persons, provided the contract calls for the export of relevant unclassified technical data, and such data are being exported only by the prime contractor. Such data shall not disclose the details of development, engineering, design, production, or manufacture of any arms, ammunition or implements of war on the U.S. Munitions List. (This exemption does not

³The burden for obtaining appropriate U.S. Government approval for the publication of technical data falling within the definition in § 125.01, including such data as may be developed under other than U.S. Government contract, is on the person or company seeking publication.

§ 125.11

Title 22—Foreign Relations

permit the prime contractor to enter into subsidiary technical assistance or manufacturing license agreements, or any arrangement which calls for the exportation of technical data without compliance with Part 124 of this subchapter).

(5) If it relates to firearms not in excess of caliber .50 and ammunition for such weapons, except technical data containing advanced designs, processes, and manufacturing techniques.

(6) If it consists of technical data, other than design, development, or production information relating to equipment, the export of which has been previously authorized to the same recipient.

(7) If it consists of operations, maintenance, and training manuals, and aids relating to equipment, the export of which has been authorized to the same recipient.⁴

(8) If it consists of additional copies of technical data previously approved for export to the same recipient; or if it consists of revised copies of technical data, provided it pertains to the identical Munitions List article, and the revisions are solely editorial and do not add to the content of technology previously approved for export to the same recipient.

(9) If it consists solely of technical data being reexported to the original source of import.

(10) If the export is by the prime contractor in direct support and within the technical and/or product limitations of a "U.S. Government approved project" and the prime contractor so certifies. The Office of Munitions Control, Department of State, will verify, upon request, those projects which are "U.S. Government approved", and accord an exemption to the applicant who applies for such verification and exemption, where appropriate, under this subparagraph.⁵

⁴Not applicable to technical data relating to Category VI(e) and Category XVI.

⁵Classified information may also be transmitted in direct support of and within the technical and/or product limitations of such verified "U.S. Government approved projects" without prior Department of State approval provided the U.S. party so certifies and complies with the requirements of the

(11) If the export is solely for the use of American citizen employees of U.S. firms provided the U.S. firm certifies its overseas employee is a U.S. citizen and has a "need to know."⁶

(12) If the export is directly related to classified information, the export of which has been previously authorized to the same recipient, and does not disclose the details of design, production, or manufacture of any arms, ammunition, or implements of war on the U.S. Munitions List.

(b) *Plant visits.* Except as restricted by the provisions of § 126.01 of this subchapter:

(1) No license shall be required for the oral and visual disclosure of unclassified technical data during the course of a plant visit by foreign nationals provided the data is disclosed in connection with a classified plant visit or the visit has the approval of a U.S. Government agency having authority for the classification of information or material under Executive Order 11652, as amended, and other applicable Executive Orders and the requirements of Section V, paragraph 40(d) of the Industrial Security Manual are met.

(2) No license shall be required for the documentary disclosure of unclassified technical data during the course of a plant visit by foreign nationals provided the document does not contain technical data as defined in § 125.01 in excess of that released orally or visually during the visit, is within the terms of the approved visit request, and the person in the United States assures that the technical data

Department of Defense Industrial Security Manual relating to the transmission of such classified information (and any other requirements of cognizant U.S. Government departments or agencies).

⁶Classified information may also be exported to such certified American citizen employees without prior Department of State approval provided the U.S. party complies with the requirements of the Department of Defense Industrial Security Manual relating to the transmission of such classified information (and any other requirements of cognizant U.S. Government departments or agencies). Such technical data or information (classified or unclassified) shall not be released by oral, visual, or documentary means to any foreign person.

Chapter I—Department of State

§ 125.21

will not be used, adapted for use, or disclosed to others for the purpose of manufacture or production without the prior approval of the Department of State in accordance with Part 124 of this subchapter.

(3) No department of State approval is required for the disclosure of oral and visual classified information during the course of a plant visit by foreign nationals provided the visit has been approved by the cognizant U.S. Defense agency and the requirements of section V, paragraph 40(d) of the Defense Industrial Security Manual are met.

[Dept. Reg. 108.605, 35 FR 12037, July 17, 1969, as amended by Dept. Reg. 108.630, 35 FR 19995, Dec. 31, 1970; Dept. Reg. 108.646, 36 FR 20941, Nov. 2, 1971; Dept. Reg. 108.649, 36 FR 22741, Nov. 30, 1971; Dept. Reg. 108.668, 37 FR 14694, July 22, 1972]

§ 125.12 Canadian shipments.

District directors of customs and postal authorities are authorized to permit the export of unclassified technical data to Canada without an export license, except when such technical data relate to the following:

(a) Nuclear weapons strategic delivery systems and all specifically designed components, parts, accessories, attachments, and associated equipment therefor;

(b) Nuclear weapons design and test equipment defined in Category XVI;

(c) Naval nuclear propulsion equipment as defined in Category VI(e);

(d) Aircraft as defined in Category VIII(a); and

(e) Submersible and oceanographic vessels and related articles as defined in Category XX (a) through (d).

(This exemption does not authorize the foreign manufacture of any arms, ammunition, or implements of war on the U.S. Munitions List. See Part 124 of this subchapter.)

[Dept. Reg. 108.630, 35 FR 19995, Dec. 31, 1970, as amended by Dept. Reg. 108.646, 36 FR 20941, Nov. 2, 1971]

§ 125.13 Data on nuclear materials.

To the extent that technical data, the export of which are controlled by the Atomic Energy Commission under the Atomic Energy Act of 1954, as

amended, are coextensive with technical data related to articles in Category VI(e), Category XVI, and Category XVIII, the provisions of this subchapter shall not apply.

PROCEDURES

§ 125.20 Export of unclassified technical data.

(a) *General and visits.* Unless exempted in § 125.10 or § 125.11 of this subchapter, applications for the export or the disclosure of nonexempt unclassified technical data to foreign persons shall be made (by persons in the United States only) to the Department of State on Form DSP-5, accompanied by five copies of the data. In the case of visits, sufficient details of the proposed discussions shall be transmitted in quintuplicate for an adequate appraisal of the data in question.

(b) *Patents.* All requests for filing patent applications in a foreign country, and requests for filing amendments, modifications or supplements thereto, shall be directed to the U.S. Patent Office in accordance with 37 CFR Part 5. If the applicant complies with the regulations of the Patent Office, no approval of the Department of State is required unless the applicant seeks to export technical data exceeding that used to support a patent application in a foreign country. In such case an application shall be required to be submitted on form DSP-5 in accordance with the provisions of paragraph (a) of this section.

[Dept. Reg. 108.615, 35 FR 3030, Feb. 14, 1970, and Dept. Reg. 108.646, 36 FR 20941, Nov. 2, 1971]

§ 125.21 Export of classified information (data and equipment).

Unless exempted in § 125.10 or § 125.11, applications (from U.S. citizens only) for approval to export or disclose classified information (data or equipment) to foreign persons shall be submitted to the Department of State on form DSP-85. When the application is for export of classified technical data only it shall be accompanied by five copies of the data to permit an evaluation of whether an export li-

§ 125.22

cense may be issued. When the application is for export of classified equipment it shall be accompanied by five copies of suitable descriptive information to permit an evaluation of whether an export license may be issued, and form DSP-83 in the case of significant combat equipment (see footnote 3 to § 123.10 (d) of this subchapter). All classified materials accompanying an application shall be treated as required by the Defense Industrial Security Manual, section I, paragraph 5.

[Dept. Reg. 108.646, 36 FR 20942, Nov. 2, 1971]

§ 125.22 Certification requirements.

An exporter in the United States claiming any exemption for the export of technical data in accordance with the provisions of § 125.11, may do so by certifying that the proposed export is covered by the relevant paragraph(s) of that section. Such certification shall be made by marking the package or letter "22 CFR 125.11 * * * applicable," identifying the specific paragraph(s) under which the exemption is claimed.

§ 125.23 Filing of licenses for export of unclassified technical data.

DSP-5 licenses authorizing the export of unclassified technical data shall be presented to, and filed with the appropriate district director of customs or postmaster at the time of shipment or mailing. The district director of customs or postmaster shall endorse and transmit the licenses to the Office of Munitions Control, Department of State, in accordance with the instructions contained on the reverse thereof.

[Dept. Reg. 108.615, 35 FR 3030, Feb. 14, 1970]

§ 125.24 Filing of licenses for export of classified information (data and equipment).

DSP-85 licenses authorizing the export of classified data or classified equipment shall be forwarded by the Department of State to agents of the Department of Defense (Defense Supply Agency) to arrange for transmission in accordance with the De-

Title 22—Foreign Relations

partment of Defense Industrial Security Manual. The Department of State shall forward a copy of the issued license to the applicant for his information. Upon completion of the export transaction the Defense Supply Agency shall return the license to the Department of State with endorsements in accordance with the instructions contained on the reverse thereof.

[Dept. Reg. 108.615, 35 FR 3030, Feb. 14, 1970]

PART 126—PROHIBITED SHIPMENTS, TEMPORARY SUSPENSION OR MODIFICATION OF REGULATIONS, EXEMPTIONS, AND RELATION TO OTHER PROVISIONS OF LAW

Sec.

126.01 Prohibited shipments to or from certain countries.

126.02 Temporary suspension or modification of regulations of the subchapter.

126.03 Waiver or exception in hardship cases.

126.04 Shipments by U.S. Government agencies.

126.05 Relation to other provisions of law.

AUTHORITY: Sec. 414, as amended, 68 Stat. 848, 22 U.S.C. 1934; secs. 101 and 105, E.O. 10973, 26 FR 10469; sec. 6, Departmental Delegation of Authority No. 104, 26 FR 10608, as amended, 27 FR 9925, 28 FR 7231; Redlegation of Authority No. 104-3-A, 28 FR 7231.

SOURCE: Dept. Reg. 108.605, 34 FR 12039, July 17, 1969, unless otherwise noted.

§ 126.01 Prohibited shipments to or from certain countries.

The policy of the United States is to deny licenses and other approvals for U.S. Munitions List articles destined for or originating in Albania, Bulgaria, Communist China, Cuba, Czechoslovakia, East Germany, Estonia, Hungary, Latvia, Lithuania, North Korea, Outer Mongolia, Poland, Rumania, Union of Soviet Socialist Republics, any of the area of Viet-Nam which is under *de facto* communist control, and to or from any other area where the shipment of Munitions List articles would not be in furtherance of world peace and the security and foreign policy of the United States. The exemptions provided in the regulations in this subchapter, except § 125.11(a) (1) and (2)

EXHIBIT 12



DEPARTMENT OF STATE

Washington, D. C. 20520

MUNITIONS CONTROL NEWSLETTER

NO. 80

2/80


CRYPTOGRAPHY/TECHNICAL DATA

Concern has been voiced that ITAR provisions relating to the export of technical data as applied to cryptologic equipment can be so broadly interpreted as to restrict scientific exchanges of basic mathematical and engineering research data. The Office of Munitions Control wishes to clarify the application of the technical data provisions of Section 121.01, Category XVIII, of the ITAR as applied to equipment found in Categories XI(c) and XIII(b) of the Munitions List.

Cryptologic technical data for which a license is required under Section 121.01, Category XVIII, is interpreted by this office with respect to information relating to Munitions List items in Categories XI(c) and XIII(b) to include only such information as is designed or intended to be used, or which reasonably could be expected to be given direct application, in the design, production, manufacture, repair, overhaul, processing, engineering, development, operation, maintenance or reconstruction of items in such categories. This interpretation includes, in addition to engineering and design data, information designed or reasonably expected to be used to make such equipment more effective, such as encoding or enciphering techniques and systems, and communications or signal security techniques and guidelines, as well as other cryptographic and cryptanalytic methods and procedures. It does not include general mathematical, engineering or statistical information, not purporting to have or reasonably expected to be given direct application to equipment in such categories. It does not include basic theoretical research data. It does, however, include algorithms and other procedures purporting to have advanced cryptologic application.

The public is reminded that professional and academic presentations and informal discussions, as well as demonstrations of equipment, constituting disclosure of cryptologic technical data to foreign nationals, are prohibited without the prior approval of this office. Approval is not required for publication of data within the United States as described in Section 125.11(a)(1). Footnote 3 to section 125.11 does not establish a prepublication review requirement.

The interpretation set forth in this newsletter should exclude from the licensing provisions of the ITAR most basic scientific data and other theoretical research information, except for information intended or reasonably expected to have a direct cryptologic application. Because of concerns expressed to this office that licensing procedures for proposed disclosures of cryptologic technical data contained in professional and academic papers and oral presentations could cause burdensome delays in exchanges with foreign scientists, this office will expedite consideration as to the application of ITAR to such disclosures. If requested, we will, on an expedited basis provide an opinion as to whether any proposed disclosure, for other than commercial purposes, of information relevant to cryptology, would require licensing under the ITAR.


William B. Robinson, Director
Office of Munitions Control

Mr. INGRAM. The bottom line is that the regulations themselves have not been amended.

Mr. FOY. That is correct.

Mr. INGRAM. Let me call your attention to a letter of August 29, 1978, from your colleague, Larry Hammond, Deputy Assistant Attorney General, Office of Legal Counsel, to Col. Wayne Kay, Senior Policy Analyst, Office of Science and Technology Policy, Executive Office of the President.

The letter discusses the *Edler* case that you mentioned, which did present a first amendment challenge to the Munitions Control Act of 1954 and the ITAR. As Hammond notes, his letter to Kay is a followup to the Department's memorandum of 3 months previous to Dr. Press on public cryptography and the ITAR. Hammond goes on to conclude, at page 2 of his letter,

While the ninth circuit's decision in *Edler* is helpful in resolving first amendment issues with respect to blueprints and similar types of technical data used as a basis for producing military equipment, we do not believe that it either resolves the first amendment issues presented by restrictions on the export of cryptographic ideas or eliminates the need to reexamine the ITAR.

[The material follows:]

EXHIBIT 13

WILLIAMS MULLEN

Jahna M. Harwig
Direct Dial: 202.293-8145
jharwig@williamsmullen.com

June 21, 2013

Ms. Sarah Heidema
U.S. Department of State
Directorate of Defense Trade Controls
PM/DDTC, SA-1, Room 1200
2401 E Street, NW
Washington, DC 20037

Subject: Commodity Jurisdiction Requests for Data Files Posted by Defense Distributed

Enclosures: (1) Printouts of Drawings from Files Posted at DEFCAD.org
(2) Wikipedia Page for 125mm BK-14M HEAT
(3) Thingiverse Page for Sound Moderator
(4) Thingiverse Page for VZ-58 Front Sight
(5) Examples of Solvent Trap Adapters
(6) Examples of CAD Files for .22 Pistols
(7) Examples of CAD Files for Muzzle Brakes
(8) Examples of CAD Files for Slide Assemblies
(9) Examples of CAD Files for Voltlock System

Dear Ms. Heidema:

Defense Distributed has been requested by DTCC/END to submit requests for commodity jurisdiction determinations in connection with Case No. 13-0001444 for ten sets of data files posted to DEFCAD.org. As demonstrated below, the files are primarily Computer Aided Design (CAD) data files and should be considered public domain information that is excluded from the ITAR pursuant to Section 120.11. Defense Distributed therefore respectfully requests a determination that these files are not subject to the ITAR.

COMMODITY DESCRIPTIONS

Each of these Commodity Jurisdiction requests relates to data files, almost all of which are essentially blueprints that can be read by CAD software. A description of each file or set of files is set out below. The files are in one of the following formats:

- STL (STereoLithography or Standard Tessellation Language) is a file format native to the stereolithography CAD software and can be used with some 3D printers. "Stereolithography" is a means of creating physical 3D models of objects using resin or carefully cut and joined pieces of paper. STL files describe only

the surface geometry of a three dimensional object without any representation of color, texture or other common CAD model attributes.

- The IGS (Initial Graphics Exchange Specification) file format is the standard format for transferring three-dimensional models between CAD programs. IGS files can store wireframe models, surface or solid object representations, circuit diagrams, and other objects.
- SLDPRT is the proprietary image file format associated with the SolidWorks brand CAD software. SLDPRT files contain three-dimensional images of one specific part of a product.
- SKP is the CAD drawing format for Google Sketchup, which is a quick, entry-level 3D drawing program.

There are also a small number of Word (.DOC), text (.TXT) or image (.JPG or .BMP) files. A printout of each file is attached to the relevant DS-4076.

As explained further below, each of these files either was previously placed in the public domain or contains only public domain information.

1. Liberator Pistol Data Files

The files for the Liberator Pistol include sixteen STL files for the various parts and components of the pistol, two “read me” text files that explain how to lawfully assemble the pistol, a diagram of a pistol, and a permissive software license. If printed on a 3D printer, the parts could be assembled into a single shot .380 caliber firearm.

2. .22 Electric Data Files

The files for the .22 Electric are two stereolithography (STL) CAD files for models of a barrel and grip for a .22 caliber pistol. If printed, the barrel would be a plastic cylinder with a .22 mm bore and the grip would be a plastic piece with two 5mm diameter holes. If those pieces were printed in plastic and used with an electronic system and firing mechanism, the barrel would be expected to fail upon firing.

3. 125 mm BK-14M High Explosive Anti-Tank Warhead Model Data File

The file is a STL CAD file for a model of a BK-14M high explosive anti-tank warhead without fins. The model, if printed on a 3D printer, would be a solid piece of plastic in the shape of the warhead, but would not be capable of functioning as a warhead.

4. 5.56/.223 Muzzle Brake Data Files

The data files are three different CAD file formats (.IGS, .SLDPRT, and .STL) for a model of a 5.56/.223 muzzle brake. If printed on a 3D printer, the model would be a plastic piece in the shape of the muzzle brake, but would be expected to fail if used with a weapon.

5. Springfield XD-40 Tactical Slide Assembly Data Files

The files are nineteen Computer Aided Design (CAD) data files in the SolidWorks .SLDPRT file format for models of components of a pistol slide for the Springfield XD-40. The

components, if printed on a 3D printer, would be plastic pieces in the shape of the components of the slide assembly, but would be expected to fail if used with a weapon.

6. Sound Moderator – Slip On File

The file is a stereolithography CAD file for a model of a slip-on sound moderator for an air gun. The model, if printed on a 3D printer, would work with an air gun, but would likely melt if used with a firearm.

7. “The Dirty Diane” ½-28 to ¼-16 STP S3600 Oil Filter Silencer Adapter Files

The file is a CAD data file in the SolidWorks .SLDPRT file format for a model of an oil filter silencer adapter that is typically produced in stainless steel. If printed on a 3D printer, this item could be used as a solvent trap adapter, which is used to catch solvents that are used in the process of cleaning a gun. While a metal solvent trap adapter could be used as a silencer, a plastic adapter would likely melt if used with a weapon as a silencer.

8. 12 Gauge to .22 CB Sub-Caliber Insert Files

The files are a SKP CAD file for a model of a sub-caliber insert, two renderings of the sub-caliber insert, and a “read me” text file providing information about the National Firearms Act and the Undetectable Firearms Act. This item, if printed on a 3D printer, would be a plastic cylinder with a .22 bore, and would be expected to fail if used with a weapon.

9. Voltlock Electronic Black Powder System Files

The files are twelve CAD files for models of cylinders of various bores with a touch hole. Eleven of the files are in the STL file format and one is in the IGS format. If those pieces were printed on a 3D printer and used with an electronic ignition, the barrel would be expected to fail.

10. VZ-58 Front Sight Files

The files are a SolidWorks CAD file in the .SLDPRT file format and a rendering of a model of a sight for a VZ-58 rifle. If printed on a 3D printer and used with a weapon, the sight would be expected to fail.

DATA ORIGIN

With the exception of item 1 (Liberator Pistol Data Files), each of these files was provided to Defense Distributed by the creator of the files identified in the DS4076. In addition, as explained below, many of these files were originally posted to www.thingiverse.com or other internet sites, and were freely available to any person with access to the internet.

The Liberator Pistol CAD files were developed by Defense Distributed. The Liberator pistol was designed as a combination of already extant and working files and concepts. The pistol frame, trigger housing, and grip specifications were all taken directly from an AR-15 lower receiver file that is in the public domain. The spring file is taken from a toy car file available on Thingiverse. The hammer relies on striking a common roofing nail, and the barrel is a cylinder bored for .380. The gun functions because of the properties of the .380 cartridge – the brass

Defense Distributed CJ Requests

June 21, 2013

Page 4

casing itself is relied on to act as a breech. The printed and assembled gun is a simple improvised weapon, not as complex as many of the improvised weapons of the 20th century, those available in Army manuals, etc. All of the technologies used to create the Liberator data files are widely available in the public domain.

IDENTICAL & SIMILAR FILES

The Liberator Pistol data files are for an improvised firearm that is similar to and based on numerous items that are available on the internet as well as in various books. The Library of Congress online catalog lists numerous books on gunsmithing, including

- Clyde Baker, Modern gunsmithing; a manual of firearms design, construction, and remodeling for amateurs & professionals (1959)
- John E. Traister, Clyde Baker's Modern gunsmithing : a revision of the classic (1981)
- Frank de Haas, Mr. Single Shot's gunsmithing idea book (1983)
- Roy F. Dunlop, Gunsmithing (1996),
- Franklin Fry, Gunsmithing fundamentals : a guide for professional results (1988),
- James Virgil Howe, The modern gunsmith : a guide for the amateur and professional gunsmith in the design and construction of firearms, with practical suggestions for all who like guns (1982),
- Gérard Métral, A do-it-yourself submachine gun: it's homemade, 9mm, lightweight, durable, and it'll never be on any import ban lists! (1995),
- Jack Mitchell, The Gun digest book of pistolsmithing (1980),
- J. Parrish Stelle, The gunsmith's manual; a complete handbook for the American gunsmith (1883), and
- Patrick Sweeney, Gunsmithing: pistols & revolvers (2009),

among many others. Examples of online sources include:

- <http://www.weaponscombat.com/zip-pipe-and-pen-guns>
- <http://www.infinitearms.com/images2/v/manuals/Misc+Gun+Plans>
- <http://thehomegunsmith.com>
- <http://www.scribd.com/doc/24445441/Pen-Gun-Mk1-Blueprint>
- https://www.google.com/search?q=zip+gun+blueprints&rlz=1C1SKPM_enUS436US489&source=lnms&tbn=isch&sa=X&ei=9t-oUZybJILm8wSx0YHoBg&ved=0CAoQ_AUoAQ&biw=1600&bih=837
- <http://ebookbrowse.com/gu/guns-homemade>

Although DD converted this information into CAD file format, DD does not believe that it created any new technical data for the production of the gun.

A drawing of the 125 BK-14M HEAT (Item 3), including measurements, is currently available on Wikipedia at http://en.wikipedia.org/wiki/File:125mm_BK-14m_HEAT.JPG.

Defense Distributed CJ Requests

June 21, 2013

Page 5

The Sound Moderator CAD file (Item 6) was published on Thingiverse on March 3, 2011 and is still available on that site at <http://www.thingiverse.com/thing:6808>. The VZ-58 Front Sight (Item 10) was also published to Grabcad on December 14, 2012 and is still available on that site at <http://grabcad.com/library/front-sight-for-vz-dot-58-rifle>.

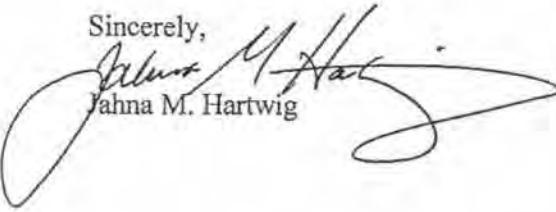
The Oil Filter Silencer Adapter is identical to Solvent Trap Adapters, which are produced by numerous manufacturers and available as commercial products on many websites, including amazon.com. (see http://www.amazon.com/s/ref=nb_sb_noss_1?url=search-alias%3Dautomotive&field-keywords=solvent+trap+adapter&rh=n%3A15684181%2Ck%3Asolvent+trap+adapter.) These items appear to be commercial products that would be subject to the EAR. As such, any related technologies or technical data would also be subject to the EAR.

Examples of CAD files similar to the .22 Electric Pistol (Item 2), Muzzle Brake (Item 4), Slide Assembly (Item 5), and Voltlock Electronic Black Powder System (Item 9) that are currently available on the internet are attached to the relevant DS4076.

As demonstrated above, all of the technical information included in the data files posted to DEFCAD.org was previously available in the public domain. As such, this information is excluded from the definition of "technical data" by 22 C.F.R. § 120.10(a)(5). For these reasons, Defense Distributed respectfully requests that the Department determine that the subject data files posted to DEFCAD.org are not subject to the ITAR.

This submission contains Defense Distributed confidential business information. We respectfully request that the submission be kept confidential. If you need additional information regarding this submission, please contact me at 202-293-8145 or jhartwig@williamsmullen.com.

Sincerely,


Jahna M. Hartwig

Electronic Form Version Number: 1.2
For DDTC Use Only
CJ Number: _____

OMB APPROVAL NO: 1405-0163
EXPIRATION DATE: 01/31/2013
*ESTIMATED BURDEN: 10 Hours

U.S. Department of State

DS-4076 Commodity Jurisdiction (CJ) Determination Form

*PAPERWORK REDUCTION ACT STATEMENT: Public reporting burden for this collection of information is estimated to average 10 hours per response, including time required for searching existing data sources, gathering the necessary data, providing the information required, and reviewing the final collection. Send comments on the accuracy of this estimate of the burden and recommendations for reducing it to: Department of State (A/CIS/DIR) Washington, D.C. 20520.

A. Applicant Information

1. Applicant's Information: (Select all that apply)

Applicant is: ☐ Government ☐ Manufacturer ☐ Exporter ☐ Manufacturer's Representative ☒ Other

Applicant Name: (Company, Organization) Defense Distributed

Address: 711 W. 32nd Street, Apt. 115

City: Austin

State: TX

Zip Code: 78705

Phone #: 501-743-9680

PM/DDTC Registrant Code: _____ (If applicable)

Add Item

Remove Item

Name: (Point of Contact) Cody R. Wilson

Phone #: 501-743-9680

Fax #: _____

Email: crw@defdist.org

2. Submitter Information if other than Applicant in Block 1: (Complete if applicable)

Submitter Name: (Company, Organization) Williams Mullen PC

Address: 1666 K St., NW, Suite 1200

City: Washington

State: DC

Zip Code: 20006

Phone #: 202-293-8145

PM/DDTC Registrant Code: _____ (If applicable)

Add Item

Remove Item

Name: (Point of Contact) Jahna M. Hartwig

Phone #: 202-293-8145

Fax #: _____

Email: jhartwig@williamsmullen.com

☒ Attachment: Authorization from Applicant to Submitter authorizing submitter to file on its behalf and to release information in Block 5.

B. Transaction Description and Compliance Information

3. Transaction Description: (Note: No request involving Classified information will be considered.)

This Application Represents:

a. ☒ New Request

b. ☐ Resubmission

Prior CJ Case Number: _____

☐ Returned Without Action (RWA)

☐ Reconsideration (Include Prior CJ Determination Case Number)

Summarize Reason for Resubmission (limited to 1200 characters)

Related to Compliance Matter (limited to 1200 characters)

☒ Yes ☐ No

If yes, provide disclosure and/or case number (if available) and details to include U.S. Government Point of Contact. If status changes advise DDTC.

DTCC Case 13-0001444. This CJ is submitted at the request of DTCC/END in its letter to Defense Distributed dated May 8, 2013. The DTCC/END Compliance Specialist is assigned to this matter is Ms. Bridget Van Buren.

C. Commodity Description

4. Select Commodity Type: (Select all that apply) (22 C.F.R. 120.9, 120.10 and 121.8)

☐ End Item

☐ Component/Major

☐ Component/Minor

☐ Part

☐ Accessory/Attachment

☐ Software

☐ Firmware

☐ Services

☐ System

☒ Information or Technical Data

5. Commodity/Service Information: (Note: Complete all that apply and if not applicable, enter "N/A".)

a. Product Name: Liberator Pistol Data Files

b. Model/Version Number: N/A

c. Part Number: N/A

d. National Stock Number: N/A

e. Other Identifier: (If applicable) N/A

f. Manufacturer: Defense Distributed

g. Service: N/A

h. Generic Description: Data files for single shot .380 caliber firearm

i. Manufacturer's Website: <u>www.defdist.org</u> j. Commodity/Service Website: <u>http://defcad.com/liberator/</u> Note: Only one commodity may be entered; variants require separate submission. However, variants of a commodity or a family of commodities closely related, that is, major characteristics and descriptive information of the commodity are essentially the same and would be included in the same U.S. Munitions List category and subcategory may be considered.	
6. Additional Commodity Information/Documentation: (Brochures, Technical Information, Drawings, Schematics, Blue Prints, Course Syllabus/Handouts, Training Materials.) Attach product datasheet or other technical information such that an informed technical evaluation is possible.) Note: cost in U.S. Dollars. If unit is not listed in drop down list, e.g. service or training, enter the commodity.	
a. Cost Per Unit:	\$0.00 _____ Copies _____ b. Documentation Attached: <input checked="" type="checkbox"/> c. Patent Information: n/a
7. Commodity/Service Description: (limited to 1200 characters) Brief summary of commodity or service (e.g. component used in aircraft communication system). Describe the product's use (what it does, how it operates, the components/system in which it is used and all current uses). Specify if commodity/service is controlled or restricted for public release by U.S. Government. <div style="border: 1px solid black; padding: 5px;"> The files for the Liberator Pistol include sixteen STL files for the various parts and components of the pistol, two "read me" text files that explain how to lawfully assemble the pistol, a diagram of a pistol, and a permissive software license. If printed on a 3D printer, the parts could be assembled into a single shot .380 caliber firearm. </div>	
8. Identify any special and/or unique characteristics/capabilities: (Mark all boxes that apply and provide explanation/description)	
a. <input type="checkbox"/> Designed to military or intelligence standards or specifications. b. <input type="checkbox"/> Designed for military application. c. <input type="checkbox"/> Special characteristics (e.g. radiation-hardening, ballistic protection, hard points, TEMPEST capability, thermal or infrared signature reduction capability, surveillance or intelligence gathering capability). d. <input type="checkbox"/> Commercial item modified for military application, provide nomenclature and model number to differentiate from commercial item. e. <input type="checkbox"/> Commercial item modified for military application, state specific distinct difference between original commercial item and modified item. f. <input type="checkbox"/> Services (provide comparable information as that which provided above and by marking this box, indicate it is for services versus hardware). Explanation/Description (If the product is included in a higher assembly or end item, identify each higher assembly or end item that incorporates the product and its use. Identify all military applications and military capabilities of the product, and any equivalent products used for military application.) Summarize technical details of special characteristics (e.g. if image intensification tubes, provide level of technology, such as Gen II, Gen III, etc.). (limited to 600 characters) <div style="border: 1px solid black; padding: 5px;">N/A</div>	
D. Product Origin	
9. Military/Commercial Modification of Commodity:	
a. Was this commodity originally specifically designed or developed for a military use? <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No b. Was this commodity originally civil and subsequently adapted, configured or modified for a military use? <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No c. Was this commodity originally military and subsequently adapted, reconfigured or modified for commercial use? <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No d. Specifically define the modifications/changes and capabilities added to the commodity. List any differences in form, fit and/or function between the modified and unmodified versions: (limited to 600 characters) <div style="border: 1px solid black; padding: 5px;">N/A</div> <input type="checkbox"/> Supporting Documentation Attached	
10. Status of Product Development: (Mark the status of the product and provide an explanation/description)	
a. <input checked="" type="checkbox"/> In Development b. <input type="checkbox"/> In Use Explanation/Description (limited to 4000 characters) <div style="border: 1px solid black; padding: 5px;"> These files have been used to produce the parts for the Liberator and the Liberator has been assembled and tested. </div> <input type="checkbox"/> Supporting Documentation Attached	
11. Funding History: (Check all that apply) Include funding source contract or subcontract number and supporting documentation.	
a. <input type="checkbox"/> USG Agency b. <input type="checkbox"/> Foreign Government Agency c. <input type="checkbox"/> U.S. or Foreign Contractor d. <input checked="" type="checkbox"/> Self Funded e. <input type="checkbox"/> University Funded Explanation/Description (limited to 600 characters) <div style="border: 1px solid black; padding: 5px;"> Defense Distributed received no funding from any outside source for the creation of the file. </div>	

☐ Supporting Documentation Attached

12. U.S. and/or Foreign Availability of Identical Products: (Enter Foreign Export Controls, if known)

☐ None

Manufacturer: John Simms

Commodity: online library of downloadable, printable books, blueprints, manuals and more concerning firearms, weaponry and combat topics

Model #: N/A

In Use/In Development: In Use

Foreign Exports Control:

 Manufacturer's Website: <http://www.weaponscombat.com/zip-pipe-and-pen-guns>

Manufacturer: Roderus Productions, LLC

Commodity: How-To information for the home/hobby gunsmith and enthusiast.

Model #: N/A

In Use/In Development: In Use

Foreign Exports Control:

 Manufacturer's Website: <http://www.homegunsmith.com/>

Manufacturer: E. Martillo

Commodity: Pen Gun MK1 Blueprint

Model #: NA

In Use/In Development: In Use

Foreign Exports Control:

 Manufacturer's Website: <http://www.scribd.com/doc/24445441/Pen-Gun-Mk1-Blueprint>

Manufacturer: Gun Doctor

Commodity: 1911 Frame blueprint

Model #: N/A

In Use/In Development: In Use

Foreign Exports Control:

 Manufacturer's Website: http://www.weaponer.net/forum/forum_posts.asp?TID=6933

Manufacturer: Infinite Arms, Inc.

Commodity: Silenced .22 Pistol Blueprint

Model #: N/A

In Use/In Development: In Use

Foreign Exports Control:

 Manufacturer's Website: <http://www.infinitearms.com/images2/v/manuals/Misc+Gun+Plans>

Explanation/Description (limited to 600 characters)

These are examples of public domain gun blueprints and information regarding home gunsmithing. Additional information is available in the attached letter.

☒ Supporting Documentation Attached

E. Sales Information
13. Sales Information: (Select One) (See Block 13 Template)

Military and commercial sales data must be provided, as well as listing of the military and commercial customers. The information pertains specifically to the commodity/service in Block 8. Complete the attachment, if applicable. (Note: Submit one single file up to 35MB with sales information. Do not separate the sales information into multiple smaller files.)

☐ Sales Information Attachment (Template "Block 13 Sales Information") Attached

☒ No Sales

F. Miscellaneous Information
14. Has this Commodity been: (limited to 100 characters)

a. Has this Commodity been Previously Exported

☒ Yes ☐ No ☐ Unknown

If yes, cite U.S. Government licensing jurisdiction and provide license number, if applicable.

Posted to the internet as public domain information.

b. Has this Commodity been the subject of a Prior CJ?

☐ Yes ☐ No ☒ Unknown

If yes, Cite CJ Number.

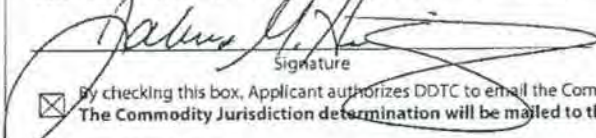
(Applicant should list any prior CJ even if not submitted by them, e.g., submitted by Original Equipment Manufacturer (OEM), by the U.S. Government or by a third party.)

c. Has this Commodity been subject to a Department of Commerce Classification Request? If yes, cite U.S. Government licensing jurisdiction and if under Department of Commerce, attach a copy with Export Control Classification Number (ECCN).	<input type="checkbox"/> Yes <input type="checkbox"/> No <input checked="" type="checkbox"/> Unknown
d. Has this Commodity been Exported under a Foreign Military Sale (FMS) case? If yes, cite Foreign Military Sale (FMS) case number.	<input type="checkbox"/> Yes <input type="checkbox"/> No <input checked="" type="checkbox"/> Unknown
15. Description of the commodity and final DDTC action will be posted on the DDTC website for public access based on the information provided in Block 5 and any other descriptive information provided below. If you believe that any information contained in Block 5 is proprietary, please specifically identify the information below and provide summarized rationale for DDTC to consider withholding the information from public notice: (Limited to 600 characters. Additional justification may be provided as an attachment.)	
N/A	
16. Reason for Submitting CJ: (limited to 600 characters)	
Per request of DTCC/END, Case No. 13-0001444.	
17. Suggested U.S. Munitions List or Commerce Control List Number:	
a. U.S. Munitions List (22 C.F.R. 121) Category/Sub Category	
N/A	
b. Export Administration Regulations (15 C.F.R. 730-774), Export Control Classification Number	
N/A	
18. Other Miscellaneous Information to be Considered that is not Otherwise Included in this Form: (e.g. U.S. Government Agency and point of contact information.) (limited to 300 characters)	
<input checked="" type="checkbox"/> Supporting Documentation Attached	

G. Applicant/Submitter's Certification

19. Applicant/Submitter's Certification: Note: ONLY this one page must be printed, signed, and scanned as an attachment.
Under Penalty According to Federal Law (See 22 CFR 127, 22 U.S.C. 2778, and 22 U.S.C. 1001).

I am the authorized employee of the company cited in Block 1, or a third party as described in Block 2 authorized to submit on behalf of the company in Block 4, and certify as to the accuracy and completeness of the information provided and have not knowingly omitted information that could have an impact on the final determination issued by the U.S. Department of State. Furthermore, I have specific authority to release for publication the text contained in Block 5.

		Jahna M. Hartwig	06/21/2013
Signature		Printed Name	Date
<input checked="" type="checkbox"/> By checking this box, Applicant authorizes DDTC to email the Commodity Jurisdiction determination as well as any other information associated with this case. The Commodity Jurisdiction determination will be mailed to the address below if box is not checked.			
Name: <u>Jahna M. Hartwig</u>			
Title: <u>Partner</u>			
Company: <u>Williams Mullen PC</u>			
Address: <u>1666 K St., NW, Suite 1200</u>			
City: <u>Washington</u>	State: <u>DC</u>	Zip Code: <u>20006</u>	
Phone #: <u>202-293-8145</u>	Email: <u>jhartwig@williamsmullen.com</u>		

Electronic Form Version Number: 1.2
For DDTC Use Only
CJ Number: _____

OMB APPROVAL NO. 1405-0163
EXPIRATION DATE: 01/31/2013
*ESTIMATED BURDEN: 10 Hours

U.S. Department of State

DS-4076 Commodity Jurisdiction (CJ) Determination Form

*PAPERWORK REDUCTION ACT STATEMENT: Public reporting burden for this collection of information is estimated to average 10 hours per response, including time required for searching existing data sources, gathering the necessary data, providing the information required, and reviewing the final collection. Send comments on the accuracy of this estimate of the burden and recommendations for reducing it to: Department of State (A/GIS/DIR) Washington, D.C. 20520.

A. Applicant Information

1. Applicant's Information: (Select all that apply)

Applicant is: ☐ Government ☐ Manufacturer ☐ Exporter ☐ Manufacturer's Representative ☒ Other

Applicant Name: (Company, Organization) Defense Distributed

Address: 711 W. 32nd Street, Apt. 115

City: Austin

State: TX

Zip Code: 78705

Phone #: 501-743-9680

PM/DDTC Registrant Code: _____

(If applicable)

Add Item

Remove Item

Name: (Point of Contact) Cody R. Wilson

Phone #: 501-743-9680

Fax #: _____

Email: crw@defdist.org

2. Submitter Information if other than Applicant in Block 1: (Complete if applicable)

Submitter Name: (Company, Organization) Williams Mullen PC

Address: 1666 K St., NW, Suite 1200

City: Washington

State: DC

Zip Code: 20006

Phone #: 202-293-8145

PM/DDTC Registrant Code: _____

(If applicable)

Add Item

Remove Item

Name: (Point of Contact) Jahna M. Hartwig

Phone #: 202-293-8145

Fax #: _____

Email: jhartwig@williamsmullen.com

☒ Attachment: Authorization from Applicant to Submitter authorizing submitter to file on its behalf and to release information in Block 5.

B. Transaction Description and Compliance Information

3. Transaction Description: (Note: No request involving Classified information will be considered.)

This Application Represents:

a. ☒ New Request

b. ☐ Resubmission

Prior CJ Case Number: _____

☐ Returned Without Action (RWA)

☐ Reconsideration (Include Prior CJ Determination Case Number)

Summarize Reason for Resubmission (limited to 1200 characters)

Related to Compliance Matter (limited to 1200 characters)

☒ Yes ☐ No

If yes, provide disclosure and/or case number (if available) and details to include U.S. Government Point of Contact. If status changes advise DDTC.

DTCC Case 13-0001444. This CJ is submitted at the request of DTCC/END in its letter to Defense Distributed dated May 8, 2013. The DTCC/END Compliance Specialist is assigned to this matter is Ms. Bridget Van Buren.

C. Commodity Description

4. Select Commodity Type: (Select all that apply) (22 C.F.R. 120.9, 120.10 and 121.8)

☐ End Item

☐ Component/Major

☐ Component/Minor

☐ Part

☐ Accessory/Attachment

☐ Software

☐ Firmware

☐ Services

☐ System

☒ Information or Technical Data

5. Commodity/Service Information: (Note: Complete all that apply and if not applicable, enter "N/A".)

a. Product Name: .22 Electric Data Files

b. Model/Version Number: N/A

c. Part Number: N/A

d. National Stock Number: N/A

e. Other Identifier: (If applicable) N/A

f. Manufacturer: Proteus

g. Service: N/A

h. Generic Description: STL data files for plastic model of barrel and grip pieces for .22 electric firearm

i. Manufacturer's Website: <u>www.defdist.org</u>	
j. Commodity/Service Website: <u>http://defcad.com/capacitor-22-firearm/</u>	
Note: Only one commodity may be entered; variants require separate submission. However, variants of a commodity or a family of commodities closely related, that is, major characteristics and descriptive information of the commodity are essentially the same and would be included in the same U.S. Munitions List category and subcategory may be considered.	
6. Additional Commodity Information/Documentation: (Brochures, Technical Information, Drawings, Schematics, Blue Prints, Course Syllabus/Handouts, Training Materials.) Attach product datasheet or other technical information such that an informed technical evaluation is possible.) Note: cost in U.S. Dollars. If unit is not listed in drop down list, e.g. service or training, enter the commodity.	
a. Cost Per Unit: <u>50.00</u>	Copies <u> </u>
b. Documentation Attached: <input checked="" type="checkbox"/>	
c. Patent Information: <u>n/a</u>	
7. Commodity/Service Description: (limited to 1200 characters) Brief summary of commodity or service (e.g. component used in aircraft communication system). Describe the product's use (what it does, how it operates, the components/system in which it is used and all current uses). Specify if commodity/service is controlled or restricted for public release by U.S. Government. The files are two stereolithography CAD files that are models of a barrel and grip for a .22 caliber pistol. If printed, the barrel would be a plastic cylinder with a .22 mm bore and the grip would be a plastic piece with two 5mm diameter holes. If those pieces were printed in plastic and used with an electronic system and firing mechanism, the barrel would be expected to fail upon firing.	
8. Identify any special and/or unique characteristics/capabilities: (Mark all boxes that apply and provide explanation/description)	
a. <input type="checkbox"/> Designed to military or intelligence standards or specifications. b. <input type="checkbox"/> Designed for military application. c. <input type="checkbox"/> Special characteristics (e.g. radiation-hardening, ballistic protection, hard points, TEMPEST capability, thermal or infrared signature reduction capability, surveillance or intelligence gathering capability). d. <input type="checkbox"/> Commercial item modified for military application, provide nomenclature and model number to differentiate from commercial item. e. <input type="checkbox"/> Commercial item modified for military application, state specific distinct difference between original commercial item and modified item. f. <input type="checkbox"/> Services (provide comparable information as that which provided above and by marking this box, indicate it is for services versus hardware). Explanation/Description (If the product is included in a higher assembly or end item, identify each higher assembly or end item that incorporates the product and its use. Identify all military applications and military capabilities of the product, and any equivalent products used for military application.) Summarize technical details of special characteristics (e.g. if image intensification tubes, provide level of technology, such as Gen II, Gen III, etc.). (limited to 600 characters) <u>N/A</u>	
D. Product Origin	
9. Military/Commercial Modification of Commodity:	
a. Was this commodity originally specifically designed or developed for a military use? <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No	
b. Was this commodity originally civil and subsequently adapted, configured or modified for a military use? <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No	
c. Was this commodity originally military and subsequently adapted, reconfigured or modified for commercial use? <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No	
d. Specifically define the modifications/changes and capabilities added to the commodity. List any differences in form, fit and/or function between the modified and unmodified versions: (limited to 600 characters) <u>N/A</u>	
<input type="checkbox"/> Supporting Documentation Attached	
10. Status of Product Development: (Mark the status of the product and provide an explanation/description)	
a. <input checked="" type="checkbox"/> In Development b. <input type="checkbox"/> In Use Explanation/Description (limited to 4000 characters) <u>To the best of Defense Distributed's knowledge, this file is conceptual in nature and has not been used to produce the plastic models of the barrel or grip.</u>	
<input type="checkbox"/> Supporting Documentation Attached	
11. Funding History: (Check all that apply) Include funding source contract or subcontract number and supporting documentation.	
a. <input type="checkbox"/> USG Agency b. <input type="checkbox"/> Foreign Government Agency c. <input type="checkbox"/> U.S. or Foreign Contractor d. <input checked="" type="checkbox"/> Self Funded e. <input type="checkbox"/> University Funded Explanation/Description (limited to 600 characters) <u>To the best of Defense Distributed's knowledge, Proteus received no funding from any outside source for the creation of the file.</u>	

<input type="checkbox"/> Supporting Documentation Attached	
12. U.S. and/or Foreign Availability of Identical Products: (Enter Foreign Export Controls, if known)	
<input type="checkbox"/> None	<input type="button" value="Add Item"/>
<input type="button" value="Remove Item"/>	
Manufacturer: Allan Howard	
Commodity: Ruger kmkiii6 stainless steel .22 automatic pistol with 6" barrel CAD Files	
Model #: N/A	In Use/In Development: In Use
Foreign Exports Control:	
Manufacturer's Website: http://grabcad.com/library/ruger-kmkiii6-stainless-steel-22-automatic-pistol-with-6-barrel	
<input type="button" value="Remove Item"/>	
Manufacturer: Tom Prex	
Commodity: .22lr Pistol CAD Files	
Model #: N/A	In Use/In Development: In Use
Foreign Exports Control:	
Manufacturer's Website: http://grabcad.com/library/22lr-pistol	
<input type="button" value="Remove Item"/>	
Manufacturer: Fred Works	
Commodity: Browning Buck Mark Threaded Barrel	
Model #: N/A	In Use/In Development: In Use
Foreign Exports Control:	
Manufacturer's Website: http://grabcad.com/library/browning-buck-mark-threaded-barrel	
Explanation/Description (limited to 600 characters)	
These CAD files are for models of a complete .22 pistol, including the barrel and grip, as well as other components.	
<input type="checkbox"/> Supporting Documentation Attached	
E. Sales Information	
13. Sales Information: (Select One) (See Block 13 Template)	
Military and commercial sales data must be provided, as well as listing of the military and commercial customers. The information pertains specifically to the commodity/service in Block 8. Complete the attachment, if applicable. (Note: Submit one single file up to 35MB with sales information. Do not separate the sales information into multiple smaller files.)	
<input type="checkbox"/> Sales Information Attachment (Template "Block 13 Sales Information") Attached	
<input checked="" type="checkbox"/> No Sales	
F. Miscellaneous Information	
14. Has this Commodity been: (limited to 100 characters)	
a. Has this Commodity been Previously Exported <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Unknown	
If yes, cite U.S. Government licensing jurisdiction and provide license number, if applicable.	
Posted to the internet as public domain information.	
b. Has this Commodity been the subject of a Prior CJ? <input type="checkbox"/> Yes <input type="checkbox"/> No <input checked="" type="checkbox"/> Unknown	
If yes, Cite CJ Number.	
(Applicant should list any prior CJ even if not submitted by them, e.g., submitted by Original Equipment Manufacturer (OEM), by the U.S. Government or by a third party.)	
c. Has this Commodity been subject to a Department of Commerce Classification Request? <input type="checkbox"/> Yes <input type="checkbox"/> No <input checked="" type="checkbox"/> Unknown	
If yes, cite U.S. Government licensing jurisdiction and if under Department of Commerce, attach a copy with Export Control Classification Number (ECCN).	
d. Has this Commodity been Exported under a Foreign Military Sale (FMS) case? <input type="checkbox"/> Yes <input type="checkbox"/> No <input checked="" type="checkbox"/> Unknown	
If yes, cite Foreign Military Sale (FMS) case number.	
15. Description of the commodity and final DDTC action will be posted on the DDTC website for public access based on the information provided in Block 5 and any other descriptive information provided below. If you believe that any information contained in Block 5 is proprietary, please specifically identify the information below and provide summarized rationale for DDTC to consider withholding the information from public notice: (Limited to 600 characters. Additional justification may be provided as an attachment.)	
N/A	
16. Reason for Submitting CJ: (limited to 600 characters)	
Per request of DTCC/END, Case No. 13-0001444.	

17. Suggested U.S. Munitions List or Commerce Control List Number:

a. U.S. Munitions List (22 C.F.R. 121) Category/Sub Category

N/A

b. Export Administration Regulations (15 C.F.R. 730-774), Export Control Classification Number

N/A

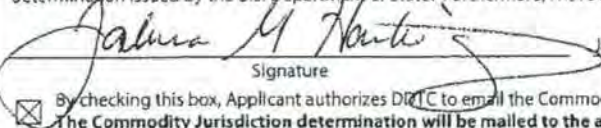
18. Other Miscellaneous Information to be Considered that is not Otherwise Included in this Form: (e.g. U.S. Government Agency and point of contact information.)
(limited to 300 characters)

☒ Supporting Documentation Attached

G. Applicant/Submitter's Certification**19. Applicant/Submitter's Certification:** Note: ONLY this one page must be printed, signed, and scanned as an attachment.

Under Penalty According to Federal Law (See 22 CFR 127, 22 U.S.C. 2778, and 22 U.S.C. 1001).

I am the authorized employee of the company cited in Block 1, or a third party as described in Block 2 authorized to submit on behalf of the company in Block 4, and certify as to the accuracy and completeness of the information provided and have not knowingly omitted information that could have an impact on the final determination issued by the U.S. Department of State. Furthermore, I have specific authority to release for publication the text contained in Block 5.



Signature

Jahna M. Hartwig

Printed Name

06/21/2013

Date

☒ By checking this box, Applicant authorizes DITC to email the Commodity Jurisdiction determination as well as any other information associated with this case.
☐ The Commodity Jurisdiction determination will be mailed to the address below if box is not checked.

Name: Jahna M. Hartwig

Title: Partner

Company: Williams Mullen PC

Address: 1666 K St., NW, Suite 1200

City: Washington

State: DC

Zip Code: 20006

Phone #: 202-293-8145

Email: jhartwig@williamsmullen.com

Electronic Form Version Number: 1.2
For DDTC Use Only
CJ Number: _____

OMB APPROVAL NO: 1405-0163
EXPIRATION DATE: 01/31/2013
*ESTIMATED BURDEN: 10 Hours

U.S. Department of State

DS-4076 Commodity Jurisdiction (CJ) Determination Form

*PAPERWORK REDUCTION ACT STATEMENT: Public reporting burden for this collection of information is estimated to average 10 hours per response, including time required for searching existing data sources, gathering the necessary data, providing the information required, and reviewing the final collection. Send comments on the accuracy of this estimate of the burden and recommendations for reducing it to: Department of State (A/GIS/DIR) Washington, D.C. 20520.

A. Applicant Information

1. Applicant's Information: (Select all that apply)

Applicant is: ☐ Government ☐ Manufacturer ☐ Exporter ☐ Manufacturer's Representative ☒ Other

Applicant Name: (Company, Organization) Defense Distributed

Address: 711 W. 32nd Street, Apt. 115

City: Austin

State: TX

Zip Code: 78705

Phone #: 501-743-9680

PM/DDTC Registrant Code: _____

(If applicable)

Add Item

Remove Item

Name: (Point of Contact) Cody R. Wilson

Phone #: 501-743-9680

Fax #: _____

Email: crw@defdist.org

2. Submitter Information if other than Applicant in Block 1: (Complete if applicable)

Submitter Name: (Company, Organization) Williams Mullen PC

Address: 1666 K St., NW, Suite 1200

City: Washington

State: DC

Zip Code: 20006

Phone #: 202-293-8145

PM/DDTC Registrant Code: _____

(If applicable)

Add Item

Remove Item

Name: (Point of Contact) Jahna M. Hartwig

Phone #: 202-293-8145

Fax #: _____

Email: jhartwig@williamsmullen.com

☐ Attachment: Authorization from Applicant to Submitter authorizing submitter to file on its behalf and to release information in Block 5.

B. Transaction Description and Compliance Information

3. Transaction Description: (Note: No request involving Classified information will be considered.)

This Application Represents:

a. ☒ New Request

b. ☐ Resubmission

Prior CJ Case Number: _____

☐ Returned Without Action (RWA)

☐ Reconsideration (Include Prior CJ Determination Case Number)

Summarize Reason for Resubmission (limited to 1200 characters)

Related to Compliance Matter (limited to 1200 characters)

☒ Yes ☐ No

If yes, provide disclosure and/or case number (if available) and details to include U.S. Government Point of Contact. If status changes advise DDTC.

DTCC Case 13-0001444. This CJ is submitted at the request of DTCC/END in its letter to Defense Distributed dated May 8, 2013. The DTCC/END Compliance Specialist is assigned to this matter is Ms. Bridget Van Buren.

C. Commodity Description

4. Select Commodity Type: (Select all that apply) (22 C.F.R. 120.9, 120.10 and 121.6)

☐ End Item

☐ Component/Major

☐ Component/Minor

☐ Part

☐ Accessory/Attachment

☐ Software

☐ Firmware

☐ Services

☐ System

☒ Information or Technical Data

5. Commodity/Service Information: (Note: Complete all that apply and if not applicable, enter "N/A".)

a. Product Name: 125 mm BK-14M high explosive anti-tank warhead model Data File

b. Model/Version Number: N/A

c. Part Number: N/A

d. National Stock Number: N/A

e. Other Identifier: (If applicable) N/A

f. Manufacturer: Proteus

g. Service: N/A

h. Generic Description: STL data file for a plastic model of a 125mm BK-14M high explosive anti-tank warhead

i. Manufacturer's Website: <u>www.defdist.org</u>	
j. Commodity/Service Website: <u>http://defcad.com/125mm-heat/</u>	
Note: Only one commodity may be entered; variants require separate submission. However, variants of a commodity or a family of commodities closely related, that is, major characteristics and descriptive information of the commodity are essentially the same and would be included in the same U.S. Munitions List category and subcategory may be considered.	
6. Additional Commodity Information/Documentation: (Brochures, Technical Information, Drawings, Schematics, Blue Prints, Course Syllabus/Handouts, Training Materials.) Attach product datasheet or other technical information such that an informed technical evaluation is possible. Note: cost in U.S. Dollars. If unit is not listed in drop down list, e.g. service or training, enter the commodity.	
a. Cost Per Unit: <u>\$0.00</u>	Copies <u> </u>
b. Documentation Attached: <input checked="" type="checkbox"/>	
c. Patent Information: <u>n/a</u>	
7. Commodity/Service Description: (limited to 1200 characters) Brief summary of commodity or service (e.g. component used in aircraft communication system). Describe the product's use (what it does, how it operates, the components/system in which it is used and all current uses). Specify if commodity/service is controlled or restricted for public release by U.S. Government. <div style="border: 1px solid black; padding: 2px;"> The file is a STL CAD files for a model of a BK-14M high explosive anti-tank warhead without fins. The model, if printed on a 3D printer, would be a solid piece of plastic in the shape of the warhead, but would not be capable functioning as a warhead. </div>	
8. Identify any special and/or unique characteristics/capabilities: (Mark all boxes that apply and provide explanation/description)	
a. <input type="checkbox"/> Designed to military or intelligence standards or specifications. b. <input type="checkbox"/> Designed for military application. c. <input type="checkbox"/> Special characteristics (e.g. radiation-hardening, ballistic protection, hard points, TEMPEST capability, thermal or infrared signature reduction capability, surveillance or intelligence gathering capability). d. <input type="checkbox"/> Commercial item modified for military application, provide nomenclature and model number to differentiate from commercial item. e. <input type="checkbox"/> Commercial item modified for military application, state specific distinct difference between original commercial item and modified item. f. <input type="checkbox"/> Services (provide comparable information as that which provided above and by marking this box, indicate it is for services versus hardware). Explanation/Description (If the product is included in a higher assembly or end item, identify each higher assembly or end item that incorporates the product and its use. Identify all military applications and military capabilities of the product, and any equivalent products used for military application.) Summarize technical details of special characteristics (e.g. if image intensification tubes, provide level of technology, such as Gen II, Gen III, etc.). (limited to 600 characters) <div style="border: 1px solid black; padding: 2px;"> N/A </div>	
D. Product Origin	
9. Military/Commercial Modification of Commodity:	
a. Was this commodity originally specifically designed or developed for a military use? <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No	
b. Was this commodity originally civil and subsequently adapted, configured or modified for a military use? <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No	
c. Was this commodity originally military and subsequently adapted, reconfigured or modified for commercial use? <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No	
d. Specifically define the modifications/changes and capabilities added to the commodity. List any differences in form, fit and/or function between the modified and unmodified versions: (limited to 600 characters) <div style="border: 1px solid black; padding: 2px;"> N/A </div>	
<input type="checkbox"/> Supporting Documentation Attached	
10. Status of Product Development: (Mark the status of the product and provide an explanation/description)	
a. <input checked="" type="checkbox"/> In Development b. <input type="checkbox"/> In Use Explanation/Description (limited to 4000 characters) <div style="border: 1px solid black; padding: 2px;"> To the best of Defense Distributed's knowledge, this file is conceptual in nature and has not been used to produce the plastic model of the warhead. </div>	
<input type="checkbox"/> Supporting Documentation Attached	
11. Funding History: (Check all that apply) Include funding source contract or subcontract number and supporting documentation.	
a. <input type="checkbox"/> USG Agency b. <input type="checkbox"/> Foreign Government Agency c. <input type="checkbox"/> U.S. or Foreign Contractor d. <input checked="" type="checkbox"/> Self Funded e. <input type="checkbox"/> University Funded Explanation/Description (limited to 600 characters) <div style="border: 1px solid black; padding: 2px;"> To the best of Defense Distributed's knowledge, Proteus received no funding from any outside source for the creation of the file. </div>	

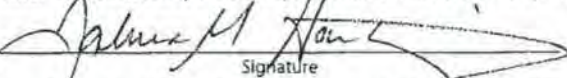
<input type="checkbox"/> Supporting Documentation Attached	
12. U.S. and/or Foreign Availability of Identical Products: (Enter Foreign Export Controls, if known)	
<input type="checkbox"/> None	<input type="button" value="Add Item"/>
<input type="button" value="Remove Item"/>	
Manufacturer: <u>Wikipedia</u>	
Commodity: <u>Data File for 125mm BK-14m HEAT Round</u>	
Model #: <u>N/A</u>	In Use/In Development: <u>In Use</u>
Foreign Exports Control: _____	
Manufacturer's Website: <u>http://en.wikipedia.org/wiki/File:125mm_BK-14m_HEAT.JPG</u>	
Explanation/Description (limited to 600 characters)	
<u>This data file contains a drawing with the dimensions for the 125mm BK14M HEAT Round along with a picture of the round.</u>	
<input checked="" type="checkbox"/> Supporting Documentation Attached	
E. Sales Information	
13. Sales Information: (Select One) (See Block 13 Template)	
Military and commercial sales data must be provided, as well as listing of the military and commercial customers. The information pertains specifically to the commodity/ service in Block 8. Complete the attachment, if applicable. (Note: Submit one single file up to 35MB with sales information. Do not separate the sales information into multiple smaller files.)	
<input type="checkbox"/> Sales Information Attachment (Template "Block 13 Sales Information") Attached	
<input checked="" type="checkbox"/> No Sales	
F. Miscellaneous Information	
14. Has this Commodity been: (limited to 100 characters)	
a. Has this Commodity been Previously Exported <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Unknown	
If yes, cite U.S. Government licensing jurisdiction and provide license number, if applicable.	
<u>Posted to the internet as public domain information.</u>	
b. Has this Commodity been the subject of a Prior CJ? <input type="checkbox"/> Yes <input type="checkbox"/> No <input checked="" type="checkbox"/> Unknown	
If yes, Cite CJ Number.	
(Applicant should list any prior CJ even if not submitted by them, e.g., submitted by Original Equipment Manufacturer (OEM), by the U.S. Government or by a third party.)	
<u>_____</u>	
c. Has this Commodity been subject to a Department of Commerce Classification Request? <input type="checkbox"/> Yes <input type="checkbox"/> No <input checked="" type="checkbox"/> Unknown	
If yes, cite U.S. Government licensing jurisdiction and if under Department of Commerce, attach a copy with Export Control Classification Number (ECCN).	
<u>_____</u>	
d. Has this Commodity been Exported under a Foreign Military Sale (FMS) case? <input type="checkbox"/> Yes <input type="checkbox"/> No <input checked="" type="checkbox"/> Unknown	
If yes, cite Foreign Military Sale (FMS) case number.	
<u>_____</u>	
15. Description of the commodity and final DDTC action will be posted on the DDTC website for public access based on the information provided in Block 5 and any other descriptive information provided below. If you believe that any information contained in Block 5 is proprietary, please specifically identify the information below and provide summarized rationale for DDTC to consider withholding the information from public notice: (Limited to 600 characters. Additional justification may be provided as an attachment.)	
<u>N/A</u>	
16. Reason for Submitting CJ: (limited to 600 characters)	
<u>Per request of DTCC/END, Case No. 13-0001444.</u>	
17. Suggested U.S. Munitions List or Commerce Control List Number:	
a. U.S. Munitions List (22 C.F.R. 121) Category/Sub Category	
<u>N/A</u>	
b. Export Administration Regulations (15 C.F.R. 730-774), Export Control Classification Number	
<u>N/A</u>	
18. Other Miscellaneous Information to be Considered that is not Otherwise Included in this Form: (e.g. U.S. Government Agency and point of contact information.) (limited to 300 characters)	
<u>_____</u>	
<input checked="" type="checkbox"/> Supporting Documentation Attached	

G. Applicant/Submitter's Certification

19. Applicant/Submitter's Certification: Note: ONLY this one page must be printed, signed, and scanned as an attachment.

Under Penalty According to Federal Law (See 22 CFR 127, 22 U.S.C. 2778, and 22 U.S.C. 1001).

I am the authorized employee of the company cited in Block 1, or a third party as described in Block 2 authorized to submit on behalf of the company in Block 4, and certify as to the accuracy and completeness of the information provided and have not knowingly omitted information that could have an impact on the final determination issued by the U.S. Department of State. Furthermore, I have specific authority to release for publication the text contained in Block 5.



Signature

Jahna M. Hartwig

Printed Name

06/21/2013

Date



By checking this box, Applicant authorizes DDTC to email the Commodity Jurisdiction determination as well as any other information associated with this case. The Commodity Jurisdiction determination will be mailed to the address below if box is not checked.

Name: Jahna M. Hartwig

Title: Partner

Company: Williams Mullen PC

Address: 1666 K St., NW, Suite 1200

City: Washington

State: DC

Zip Code: 20006

Phone #: 202-293-8145

Email: jhartwig@williamsmullen.com

Electronic Form Version Number: 1.2
For DDTC Use Only
CJ Number: _____

OMB APPROVAL NO. 1405-0163
EXPIRATION DATE: 01/31/2013
*ESTIMATED BURDEN: 10 Hours

U.S. Department of State

DS-4076 Commodity Jurisdiction (CJ) Determination Form

*PAPERWORK REDUCTION ACT STATEMENT: Public reporting burden for this collection of information is estimated to average 10 hours per response, including time required for searching existing data sources, gathering the necessary data, providing the information required, and reviewing the final collection. Send comments on the accuracy of this estimate of the burden and recommendations for reducing it to: Department of State (A/GIS/DIR) Washington, D.C. 20520.

A. Applicant Information

1. Applicant's Information: (Select all that apply)

Applicant is: ☐ Government ☐ Manufacturer ☐ Exporter ☐ Manufacturer's Representative ☒ Other

Applicant Name: (Company, Organization) Defense Distributed

Address: 711 W. 32nd Street, Apt. 115

City: Austin

State: TX

Zip Code: 78705

Phone #: 501-743-9680

PM/DDTC Registrant Code: _____

(If applicable)

Add Item

Remove Item

Name: (Point of Contact) Cody R. Wilson

Phone #: 501-743-9680

Fax #: _____

Email: crw@defdist.org

2. Submitter Information if other than Applicant in Block 1: (Complete if applicable)

Submitter Name: (Company, Organization) Williams Mullen PC

Address: 1666 K St., NW, Suite 1200

City: Washington

State: DC

Zip Code: 20006

Phone #: 202-293-8145

PM/DDTC Registrant Code: _____

(If applicable)

Add Item

Remove Item

Name: (Point of Contact) Jahna M. Hartwig

Phone #: 202-293-8145

Fax #: _____

Email: jhartwig@williamsmullen.com

☐ Attachment: Authorization from Applicant to Submitter authorizing submitter to file on its behalf and to release information in Block 5.

B. Transaction Description and Compliance Information

3. Transaction Description: (Note: No request involving Classified information will be considered.)

This Application Represents:

a. ☒ New Request

b. ☐ Resubmission

Prior CJ Case Number: _____

☐ Returned Without Action (RWA)

☐ Reconsideration (Include Prior CJ Determination Case Number)

Summarize Reason for Resubmission (limited to 1200 characters)

Related to Compliance Matter (limited to 1200 characters)

☒ Yes ☐ No

If yes, provide disclosure and/or case number (if available) and details to include U.S. Government Point of Contact. If status changes advise DDTC.

DTCC Case 13-0001444. This CJ is submitted at the request of DTCC/END in its letter to Defense Distributed dated May 8, 2013. The DTCC/END Compliance Specialist is assigned to this matter is Ms. Bridget Van Buren.

C. Commodity Description

4. Select Commodity Type: (Select all that apply) (22 C.F.R. 120.9, 120.10 and 121.8)

☐ End Item

☐ Component/Major

☐ Component/Minor

☐ Part

☐ Accessory/Attachment

☐ Software

☐ Firmware

☐ Services

☐ System

☒ Information or Technical Data

5. Commodity/Service Information: (Note: Complete all that apply and if not applicable, enter "N/A".)

a. Product Name: 5.56/.223 Muzzle Brake Data Files

b. Model/Version Number: N/A

c. Part Number: N/A

d. National Stock Number: N/A

e. Other Identifier: (If applicable) N/A

f. Manufacturer: Shane Naughton

g. Service: N/A

h. Generic Description: Three CAD data files for a 5.56/.223 muzzle brake

i. Manufacturer's Website: <u>www.defdist.org</u> j. Commodity/Service Website: <u>http://defcad.com/5-56-223-muzzle-break/</u> Note: Only one commodity may be entered; variants require separate submission. However, variants of a commodity or a family of commodities closely related, that is, major characteristics and descriptive information of the commodity are essentially the same and would be included in the same U.S. Munitions List category and subcategory may be considered.	
6. Additional Commodity Information/Documentation: (Brochures, Technical Information, Drawings, Schematics, Blue Prints, Course Syllabus/Handouts, Training Materials.) Attach product datasheet or other technical information such that an informed technical evaluation is possible. Note: cost in U.S. Dollars. If unit is not listed in drop down list, e.g. service or training, enter the commodity.	
a. Cost Per Unit: <u>\$0.00</u> Copies <u> </u> b. Documentation Attached: <input checked="" type="checkbox"/> c. Patent Information: <u>n/a</u>	
7. Commodity/Service Description: <i>(limited to 1200 characters)</i> Brief summary of commodity or service (e.g. component used in aircraft communication system). Describe the product's use (what it does, how it operates, the components/system in which it is used and all current uses). Specify if commodity/service is controlled or restricted for public release by U.S. Government. <div style="border: 1px solid black; padding: 2px;"> The data files are three different CAD file formats (.IGS, .SLDPRT, and .STL) for a model of a 5.56/.223 muzzle brake. If printed on a 3D printer, the model would be a plastic piece in the shape of the muzzle brake, but would be expected to fail if used with a weapon. </div>	
8. Identify any special and/or unique characteristics/capabilities: (Mark all boxes that apply and provide explanation/description) <ul style="list-style-type: none"> a. <input type="checkbox"/> Designed to military or intelligence standards or specifications. b. <input type="checkbox"/> Designed for military application. c. <input type="checkbox"/> Special characteristics (e.g. radiation-hardening, ballistic protection, hard points, TEMPEST capability, thermal or infrared signature reduction capability, surveillance or intelligence gathering capability). d. <input type="checkbox"/> Commercial item modified for military application, provide nomenclature and model number to differentiate from commercial item. e. <input type="checkbox"/> Commercial item modified for military application, state specific distinct difference between original commercial item and modified item. f. <input type="checkbox"/> Services (provide comparable information as that which provided above and by marking this box, indicate it is for services versus hardware). Explanation/Description (If the product is included in a higher assembly or end item, identify each higher assembly or end item that incorporates the product and its use. Identify all military applications and military capabilities of the product, and any equivalent products used for military application.) Summarize technical details of special characteristics (e.g. if image intensification tubes, provide level of technology, such as Gen II, Gen III, etc.). <i>(limited to 600 characters)</i> <div style="border: 1px solid black; padding: 2px;"> N/A </div>	
D. Product Origin	
9. Military/Commercial Modification of Commodity: <ul style="list-style-type: none"> a. Was this commodity originally specifically designed or developed for a military use? <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No b. Was this commodity originally civil and subsequently adapted, configured or modified for a military use? <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No c. Was this commodity originally military and subsequently adapted, reconfigured or modified for commercial use? <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No d. Specifically define the modifications/changes and capabilities added to the commodity. List any differences in form, fit and/or function between the modified and unmodified versions: <i>(limited to 600 characters)</i> <div style="border: 1px solid black; padding: 2px;"> N/A </div> <input type="checkbox"/> Supporting Documentation Attached	
10. Status of Product Development: (Mark the status of the product and provide an explanation/description) <ul style="list-style-type: none"> a. <input checked="" type="checkbox"/> In Development b. <input type="checkbox"/> In Use Explanation/Description <i>(limited to 4000 characters)</i> <div style="border: 1px solid black; padding: 2px;"> To the best of Defense Distributed's knowledge, this file is conceptual in nature and has not been used to produce the plastic model of the muzzle brake. </div> <input type="checkbox"/> Supporting Documentation Attached	
11. Funding History: (Check all that apply) Include funding source contract or subcontract number and supporting documentation. <ul style="list-style-type: none"> a. <input type="checkbox"/> USG Agency b. <input type="checkbox"/> Foreign Government Agency c. <input type="checkbox"/> U.S. or Foreign Contractor d. <input checked="" type="checkbox"/> Self Funded e. <input type="checkbox"/> University Funded Explanation/Description <i>(limited to 600 characters)</i> <div style="border: 1px solid black; padding: 2px;"> To the best of Defense Distributed's knowledge, Shane Naughton received no funding from any outside source for the creation of the file. </div>	

☐ Supporting Documentation Attached

12. U.S. and/or Foreign Availability of Identical Products: (Enter Foreign Export Controls, if known)

☐ None

Add Item

Remove Item

Manufacturer: Reimo SoosaarCommodity: Muzzle brake for vz.58 CAD fileModel #: N/AIn Use/In Development: In Use

Foreign Exports Control: _____

Manufacturer's Website: http://grabcad.com/library/muzzle-brake-for-vz-58

Remove Item

Manufacturer: Sam D.Commodity: 7.62mm muzzle brake (compensator)Model #: N/AIn Use/In Development: In Use

Foreign Exports Control: _____

Manufacturer's Website: http://grabcad.com/library/7-62mm-muzzle-brake-compensator

Remove Item

Manufacturer: Brett DesilvaCommodity: Mz1 brakeModel #: N/AIn Use/In Development: In Use

Foreign Exports Control: _____

Manufacturer's Website: http://grabcad.com/library/mz1-brake

Remove Item

Manufacturer: ToddAhoCommodity: Amd 65/ak 47 muzzle brakeModel #: N/AIn Use/In Development: In Use

Foreign Exports Control: _____

Manufacturer's Website: http://grabcad.com/library/amd-65-ak-47-muzzle-brake

Remove Item

Manufacturer: John ReeseCommodity: Barret m82a1Model #: N/AIn Use/In Development: In Use

Foreign Exports Control: _____

Manufacturer's Website: http://grabcad.com/library/barret-m82a1

Remove Item

Manufacturer: John ReeseCommodity: M95 muzzle brakeModel #: N/AIn Use/In Development: In Use

Foreign Exports Control: _____

Manufacturer's Website: http://grabcad.com/library/m95-muzzle-brake

Remove Item

Manufacturer: Reimo SoosaarCommodity: Muzzle brakeModel #: N/AIn Use/In Development: In Use

Foreign Exports Control: _____

Manufacturer's Website: http://grabcad.com/library/muzzle-brake

Remove Item

Manufacturer: Cody HulettCommodity: Mosin nagant m44 muzzle brakeModel #: N/AIn Use/In Development: In Use

Foreign Exports Control: _____

Manufacturer's Website: http://grabcad.com/library/mosin-nagant-m44-muzzle-brake

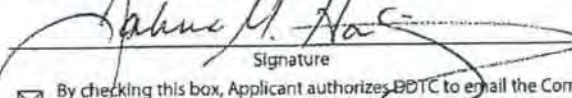
Remove Item	
Manufacturer:	Robert Ronstad
Commodity:	Suppressor 7mm
Model #:	N/A In Use/In Development: In Use
Foreign Exports Control:	
Manufacturer's Website:	http://grabcad.com/library/suppressor-7mm
Remove Item	
Manufacturer:	Justin Riegel
Commodity:	50 cal muzzle brake
Model #:	N/A In Use/In Development: In Use
Foreign Exports Control:	
Manufacturer's Website:	http://grabcad.com/library/50-cal-muzzle-brake
Remove Item	
Manufacturer:	Klaus Falk Hansen (klunk4real)
Commodity:	SolidWorks Tutorial: Muzzle Brake
Model #:	N/A In Use/In Development: In Use
Foreign Exports Control:	
Manufacturer's Website:	http://solidworks.cad2design.com/videos/196815/SolidWorks+tutorial+Muzzle+brake
Explanation/Description (limited to 600 characters)	
These CAD files contain drawings for models of various muzzle brakes. Item #13 is a video that explains how to design a muzzle brake using SolidWorks, a CAD design program.	
<input checked="" type="checkbox"/> Supporting Documentation Attached	
E. Sales Information	
13. Sales Information: (Select One) (See Block 13 Template)	
Military and commercial sales data must be provided, as well as listing of the military and commercial customers. The information pertains specifically to the commodity/service in Block 8. Complete the attachment, if applicable. (Note: Submit one single file up to 35MB with sales information. Do not separate the sales information into multiple smaller files.)	
<input type="checkbox"/> Sales Information Attachment (Template "Block 13 Sales Information") Attached	
<input checked="" type="checkbox"/> No Sales	
F. Miscellaneous Information	
14. Has this Commodity been: (limited to 100 characters)	
a. Has this Commodity been Previously Exported	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Unknown
If yes, cite U.S. Government licensing jurisdiction and provide license number, if applicable.	
Posted to the internet as public domain information.	
b. Has this Commodity been the subject of a Prior CJ?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input checked="" type="checkbox"/> Unknown
If yes, Cite CJ Number.	
(Applicant should list any prior CJ even if not submitted by them, e.g., submitted by Original Equipment Manufacturer (OEM), by the U.S. Government or by a third party.)	
c. Has this Commodity been subject to a Department of Commerce Classification Request?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input checked="" type="checkbox"/> Unknown
If yes, cite U.S. Government licensing jurisdiction and if under Department of Commerce, attach a copy with Export Control Classification Number (ECCN).	
d. Has this Commodity been Exported under a Foreign Military Sale (FMS) case?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input checked="" type="checkbox"/> Unknown
If yes, cite Foreign Military Sale (FMS) case number.	
15. Description of the commodity and final DDTC action will be posted on the DDTC website for public access based on the information provided in Block 5 and any other descriptive information provided below. If you believe that any information contained in Block 5 is proprietary, please specifically identify the information below and provide summarized rationale for DDTC to consider withholding the information from public notice: (Limited to 600 characters. Additional justification may be provided as an attachment.)	
N/A	
16. Reason for Submitting CJ: (limited to 600 characters)	
Per request of DTCC/END, Case No. 13-0001444.	
17. Suggested U.S. Munitions List or Commerce Control List Number:	
a. U.S. Munitions List (22 C.F.R. 121) Category/Sub Category	N/A

b. Export Administration Regulations (15 C.F.R. 730-774), Export Control Classification Number
N/A
18. Other Miscellaneous Information to be Considered that is not Otherwise Included in this Form: (e.g. U.S. Government Agency and point of contact information.) (limited to 300 characters)
<input checked="" type="checkbox"/> Supporting Documentation Attached

G. Applicant/Submitter's Certification

19. Applicant/Submitter's Certification: Note: ONLY this one page must be printed, signed, and scanned as an attachment.
Under Penalty According to Federal Law (See 22 CFR 127, 22 U.S.C. 2778, and 22 U.S.C. 1001).

I am the authorized employee of the company cited in Block 1, or a third party as described in Block 2 authorized to submit on behalf of the company in Block 4, and certify as to the accuracy and completeness of the information provided and have not knowingly omitted information that could have an impact on the final determination issued by the U.S. Department of State. Furthermore, I have specific authority to release for publication the text contained in Block 5.

 Signature Jahna M. Hartwig Printed Name 06/21/2013 Date

☒ By checking this box, Applicant authorizes DDTC to email the Commodity Jurisdiction determination as well as any other information associated with this case.
The Commodity Jurisdiction determination will be mailed to the address below if box is not checked.

Name: Jahna M. Hartwig
Title: Partner
Company: Williams Mullen PC
Address: 1666 K St., NW, Suite 1200
City: Washington State: DC Zip Code: 20006
Phone #: 202-293-8145 Email: jhartwig@williamsmullen.com

Electronic Form Version Number: 1.2
For DDTC Use Only
CJ Number: _____

OMB APPROVAL NO. 1405-0163
EXPIRATION DATE: 01/31/2013
*ESTIMATED BURDEN: 10 Hours

U.S. Department of State

DS-4076 Commodity Jurisdiction (CJ) Determination Form

*PAPERWORK REDUCTION ACT STATEMENT: Public reporting burden for this collection of information is estimated to average 10 hours per response, including time required for searching existing data sources, gathering the necessary data, providing the information required, and reviewing the final collection. Send comments on the accuracy of this estimate of the burden and recommendations for reducing it to: Department of State (A/GIS/DIR) Washington, D.C. 20520.

A. Applicant Information

1. Applicant's Information: (Select all that apply)

Applicant is: ☐ Government ☐ Manufacturer ☐ Exporter ☐ Manufacturer's Representative ☒ Other

Applicant Name: (Company, Organization) Defense Distributed

Address: 711 W. 32nd Street, Apt. 115

City: Austin

State: TX

Zip Code: 78705

Phone #: 501-743-9680

PM/DDTC Registrant Code: _____

(If applicable)

Add Item

Remove Item

Name: (Point of Contact) Cody R. Wilson

Phone #: 501-743-9680

Fax #: _____

Email: crw@defdist.org

2. Submitter Information if other than Applicant in Block 1: (Complete if applicable)

Submitter Name: (Company, Organization) Williams Mullen PC

Address: 1666 K St., NW, Suite 1200

City: Washington

State: DC

Zip Code: 20006

Phone #: 202-293-8145

PM/DDTC Registrant Code: _____

(If applicable)

Add Item

Remove Item

Name: (Point of Contact) Jahna M. Hartwig

Phone #: 202-293-8145

Fax #: _____

Email: jhartwig@williamsmullen.com

☐ Attachment: Authorization from Applicant to Submitter authorizing submitter to file on its behalf and to release information in Block 5.

B. Transaction Description and Compliance Information

3. Transaction Description: (Note: No request involving Classified information will be considered.)

This Application Represents:

a. ☒ New Request

b. ☐ Resubmission

Prior CJ Case Number: _____

☐ Returned Without Action (RWA)

☐ Reconsideration (Include Prior CJ Determination Case Number)

Summarize Reason for Resubmission (limited to 1200 characters)

Related to Compliance Matter (limited to 1200 characters)

☒ Yes ☐ No

If yes, provide disclosure and/or case number (if available) and details to include U.S. Government Point of Contact. If status changes advise DDTC. DTCC Case 13-0001444. This CJ is submitted at the request of DTCC/END in its letter to Defense Distributed dated May 8, 2013. The DTCC/END Compliance Specialist is assigned to this matter is Ms. Bridget Van Buren.

C. Commodity Description

4. Select Commodity Type: (Select all that apply) (22 C.F.R. 120.9, 120.10 and 121.8)

☐ End Item

☐ Component/Major

☐ Component/Minor

☐ Part

☐ Accessory/Attachment

☐ Software

☐ Firmware

☐ Services

☐ System

☒ Information or Technical Data

5. Commodity/Service Information: (Note: Complete all that apply and if not applicable, enter "N/A")

a. Product Name: Sound Moderator - Slip On Data File

b. Model/Version Number: N/A

c. Part Number: N/A

d. National Stock Number: N/A

e. Other Identifier: (If applicable) N/A

f. Manufacturer: vik

g. Service: N/A

h. Generic Description: STL file for a slip on sound moderator for an airgun

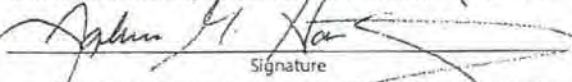
i. Manufacturer's Website:	www.defdist.org		
j. Commodity/Service Website:	http://defcad.com/sound-moderator/		
Note: Only one commodity may be entered; variants require separate submission. However, variants of a commodity or a family of commodities closely related, that is, major characteristics and descriptive information of the commodity are essentially the same and would be included in the same U.S. Munitions List category and subcategory may be considered.			
6. Additional Commodity Information/Documentation:			
(Brochures, Technical Information, Drawings, Schematics, Blue Prints, Course Syllabus/Handouts, Training Materials.) Attach product datasheet or other technical information such that an informed technical evaluation is possible. Note: cost in U.S. Dollars. If unit is not listed in drop down list, e.g. service or training, enter the commodity.			
a. Cost Per Unit:	\$0.00	Copies	
b. Documentation Attached:	<input checked="" type="checkbox"/>		
c. Patent Information:	n/a		
7. Commodity/Service Description: (limited to 1200 characters)			
Brief summary of commodity or service (e.g. component used in aircraft communication system). Describe the product's use (what it does, how it operates, the components/system in which it is used and all current uses). Specify if commodity/service is controlled or restricted for public release by U.S. Government.			
The file is a stereolithography CAD file for a model of a slip-on sound moderator for an air gun. The model, if printed on a 3D printer, would work with an air gun, but would likely melt if used with a firearm.			
8. Identify any special and/or unique characteristics/capabilities: (Mark all boxes that apply and provide explanation/description)			
a. <input type="checkbox"/> Designed to military or intelligence standards or specifications. b. <input type="checkbox"/> Designed for military application. c. <input type="checkbox"/> Special characteristics (e.g. radiation-hardening, ballistic protection, hard points, TEMPEST capability, thermal or infrared signature reduction capability, surveillance or intelligence gathering capability). d. <input type="checkbox"/> Commercial item modified for military application, provide nomenclature and model number to differentiate from commercial item. e. <input type="checkbox"/> Commercial item modified for military application, state specific distinct difference between original commercial item and modified item. f. <input type="checkbox"/> Services (provide comparable information as that which provided above and by marking this box, indicate it is for services versus hardware).			
Explanation/Description (if the product is included in a higher assembly or end item, identify each higher assembly or end item that incorporates the product and its use. Identify all military applications and military capabilities of the product, and any equivalent products used for military application.) Summarize technical details of special characteristics (e.g. if image intensification tubes, provide level of technology, such as Gen II, Gen III, etc.). (limited to 600 characters)			
N/A			
D. Product Origin			
9. Military/Commercial Modification of Commodity:			
a. Was this commodity originally specifically designed or developed for a military use?			
<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No			
b. Was this commodity originally civil and subsequently adapted, configured or modified for a military use?			
<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No			
c. Was this commodity originally military and subsequently adapted, reconfigured or modified for commercial use?			
<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No			
d. Specifically define the modifications/changes and capabilities added to the commodity. List any differences in form, fit and/or function between the modified and unmodified versions: (limited to 600 characters)			
N/A			
<input type="checkbox"/> Supporting Documentation Attached			
10. Status of Product Development: (Mark the status of the product and provide an explanation/description)			
a. <input checked="" type="checkbox"/> In Development			
b. <input type="checkbox"/> In Use			
Explanation/Description (limited to 4000 characters)			
To the best of Defense Distributed's knowledge, this file is conceptual in nature and has not been used to produce the plastic model of the sound moderator.			
<input type="checkbox"/> Supporting Documentation Attached			
11. Funding History: (Check all that apply)			
Include funding source contract or subcontract number and supporting documentation.			
a. <input type="checkbox"/> USG Agency			
b. <input type="checkbox"/> Foreign Government Agency			
c. <input type="checkbox"/> U.S. or Foreign Contractor			
d. <input checked="" type="checkbox"/> Self Funded			
e. <input type="checkbox"/> University Funded			
Explanation/Description (limited to 600 characters)			
To the best of Defense Distributed's knowledge, vik received no funding from any outside source for the creation of the file.			

<input type="checkbox"/> Supporting Documentation Attached	
12. U.S. and/or Foreign Availability of Identical Products: (Enter Foreign Export Controls, if known)	
<input type="checkbox"/> None	<input type="button" value="Add Item"/>
<input type="button" value="Remove Item"/>	
Manufacturer: <u>Vik</u>	
Commodity: <u>Sound Moderator CAD file</u>	
Model #: <u>N/A</u>	In Use/In Development: <u>In Use</u>
Foreign Exports Control: _____	
Manufacturer's Website: <u>http://www.thingiverse.com/thing:6808</u>	
Explanation/Description (limited to 600 characters)	
<u>This file was published on Thingiverse on March 3, 2011 and is still available on that site.</u>	
<input checked="" type="checkbox"/> Supporting Documentation Attached	
E. Sales Information	
13. Sales Information: (Select One) (See Block 13 Template) Military and commercial sales data must be provided, as well as listing of the military and commercial customers. The information pertains specifically to the commodity/ service in Block 8. Complete the attachment, if applicable. (Note: Submit one single file up to 35MB with sales information. Do not separate the sales information into multiple smaller files.)	
<input type="checkbox"/> Sales Information Attachment (Template "Block 13 Sales Information") Attached	
<input checked="" type="checkbox"/> No Sales	
F. Miscellaneous Information	
14. Has this Commodity been: (limited to 100 characters)	
a. Has this Commodity been Previously Exported <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Unknown If yes, cite U.S. Government licensing jurisdiction and provide license number, if applicable.	
<u>Posted to the internet as public domain information.</u>	
b. Has this Commodity been the subject of a Prior CJ? <input type="checkbox"/> Yes <input type="checkbox"/> No <input checked="" type="checkbox"/> Unknown If yes, Cite CJ Number. (Applicant should list any prior CJ even if not submitted by them, e.g., submitted by Original Equipment Manufacturer (OEM), by the U.S. Government or by a third party.)	
<u>_____</u>	
c. Has this Commodity been subject to a Department of Commerce Classification Request? <input type="checkbox"/> Yes <input type="checkbox"/> No <input checked="" type="checkbox"/> Unknown If yes, cite U.S. Government licensing jurisdiction and if under Department of Commerce, attach a copy with Export Control Classification Number (ECCN).	
<u>_____</u>	
d. Has this Commodity been Exported under a Foreign Military Sale (FMS) case? <input type="checkbox"/> Yes <input type="checkbox"/> No <input checked="" type="checkbox"/> Unknown If yes, cite Foreign Military Sale (FMS) case number.	
<u>_____</u>	
15. Description of the commodity and final DDTC action will be posted on the DDTC website for public access based on the information provided in Block 5 and any other descriptive information provided below. If you believe that any information contained in Block 5 is proprietary, please specifically identify the information below and provide summarized rationale for DDTC to consider withholding the information from public notice: (Limited to 600 characters. Additional justification may be provided as an attachment.)	
<u>N/A</u>	
16. Reason for Submitting CJs: (limited to 600 characters)	
<u>Per request of DTCC/END, Case No. 13-0001444.</u>	
17. Suggested U.S. Munitions List or Commerce Control List Number:	
a. U.S. Munitions List (22 C.F.R. 121) Category/Sub Category	
<u>N/A</u>	
b. Export Administration Regulations (15 C.F.R. 730-774), Export Control Classification Number	
<u>N/A</u>	
18. Other Miscellaneous Information to be Considered that is not Otherwise Included in this Form: (e.g. U.S. Government Agency and point of contact information.) (limited to 300 characters)	
<u>_____</u>	
<input checked="" type="checkbox"/> Supporting Documentation Attached	

G. Applicant/Submitter's Certification

19. Applicant/Submitter's Certification: Note: ONLY this one page must be printed, signed, and scanned as an attachment.
Under Penalty According to Federal Law (See 22 CFR 127, 22 U.S.C. 2778, and 22 U.S.C. 1001).

I am the authorized employee of the company cited in Block 1, or a third party as described in Block 2 authorized to submit on behalf of the company in Block 4, and certify as to the accuracy and completeness of the information provided and have not knowingly omitted information that could have an impact on the final determination issued by the U.S. Department of State. Furthermore, I have specific authority to release for publication the text contained in Block 5.

 Signature Jahna M. Hartwig Printed Name 06/21/2013 Date

☒ By checking this box, Applicant authorizes DDTC to email the Commodity Jurisdiction determination as well as any other information associated with this case.
The Commodity Jurisdiction determination will be mailed to the address below if box is not checked.

Name: Jahna M. Hartwig

Title: Partner

Company: Williams Mullen PC

Address: 1666 K St., NW, Suite 1200

City: Washington

State: DC

Zip Code: 20006

Phone #: 202-293-8145

Email: jhartwig@williamsmullen.com

U.S. Department of State

DS-4076 Commodity Jurisdiction (CJ) Determination Form

*PAPERWORK REDUCTION ACT STATEMENT: Public reporting burden for this collection of information is estimated to average 10 hours per response, including time required for searching existing data sources, gathering the necessary data, providing the information required, and reviewing the final collection. Send comments on the accuracy of this estimate of the burden and recommendations for reducing it to: Department of State (A/GIS/DIR) Washington, D.C. 20520.

A. Applicant Information**1. Applicant's Information: (Select all that apply)**Applicant is: ☐ Government ☐ Manufacturer ☐ Exporter ☐ Manufacturer's Representative ☒ OtherApplicant Name: (Company, Organization) Defense DistributedAddress: 711 W. 32nd Street, Apt. 115City: AustinState: TXZip Code: 78705Phone #: 501-743-9680

PM/DDTC Registrant Code: _____

(If applicable)

Add Item

Remove Item

Name: (Point of Contact) Cody R. WilsonPhone #: 501-743-9680

Fax #: _____

Email: crw@defdist.org**2. Submitter Information if other than Applicant in Block 1: (Complete if applicable)**Submitter Name: (Company, Organization) Williams Mullen PCAddress: 1666 K St., NW, Suite 1200City: WashingtonState: DCZip Code: 20006Phone #: 202-293-8145

PM/DDTC Registrant Code: _____

(If applicable)

Add Item

Remove Item

Name: (Point of Contact) Jahna M. HartwigPhone #: 202-293-8145

Fax #: _____

Email: jhartwig@williamsmullen.com☐ Attachment: Authorization from Applicant to Submitter authorizing submitter to file on its behalf and to release information in Block 5.**B. Transaction Description and Compliance Information****3. Transaction Description: (Note: No request involving Classified information will be considered.)**

This Application Represents:

a. ☒ New Requestb. ☐ Resubmission

Prior CJ Case Number: _____

☐ Returned Without Action (RWA)☐ Reconsideration (Include Prior CJ Determination Case Number)

Summarize Reason for Resubmission (limited to 1200 characters)

Related to Compliance Matter (limited to 1200 characters)

☒ Yes ☐ No

If yes, provide disclosure and/or case number (if available) and details to include U.S. Government Point of Contact. If status changes advise DDTC.

DTCC Case 13-0001444. This CJ is submitted at the request of DTCC/END in its letter to Defense Distributed dated May 8, 2013. The DTCC/END Compliance Specialist is assigned to this matter is Ms. Bridget Van Buren.

C. Commodity Description**4. Select Commodity Type: (Select all that apply) (22 C.F.R. 120.9, 120.10 and 121.8)**☐ End Item☐ Component/Major☐ Component/Minor☐ Part☐ Accessory/Attachment☐ Software☐ Firmware☐ Services☐ System☒ Information or Technical Data**5. Commodity/Service Information: (Note: Complete all that apply and if not applicable, enter "N/A".)**a. Product Name: 12 Gauge to .22 CB Sub-Caliber Insert Data Filesb. Model/Version Number: N/Ac. Part Number: N/Ad. National Stock Number: N/Ae. Other Identifier: (If applicable) N/Af. Manufacturer: Pietrog. Service: N/Ah. Generic Description: SKP CAD file, renderings and text file describing a sub-caliber insert

App. 237

i. Manufacturer's Website: www.defdist.org

j. Commodity/Service Website: http://defcad.com/12-gauge-to-22-cb-sub-caliber-insert/

Note: Only one commodity may be entered; variants require separate submission. However, variants of a commodity or a family of commodities closely related, that is, major characteristics and descriptive information of the commodity are essentially the same and would be included in the same U.S. Munitions List category and subcategory may be considered.

6. Additional Commodity Information/Documentation:

(Brochures, Technical Information, Drawings, Schematics, Blue Prints, Course Syllabus/Handouts, Training Materials.) Attach product datasheet or other technical information such that an informed technical evaluation is possible.) Note: cost in U.S. Dollars. If unit is not listed in drop down list, e.g. service or training, enter the commodity.

a. Cost Per Unit: \$0.00 Copies

b. Documentation Attached: ☒

c. Patent Information: n/a

7. Commodity/Service Description: (limited to 1200 characters)

Brief summary of commodity or service (e.g. component used in aircraft communication system). Describe the product's use (what it does, how it operates, the components/system in which it is used and all current uses). Specify if commodity/service is controlled or restricted for public release by U.S. Government.

The files are a SKP CAD file for a model of a sub-caliber insert, two renderings of the sub-caliber insert, and a "read me" text file providing information about the National Firearms Act and the Undetectable Firearms Act. This item, if printed on a 3D printer, would be a plastic cylinder with a .22 bore, and would be expected to fail if used with a weapon.

8. Identify any special and/or unique characteristics/capabilities: (Mark all boxes that apply and provide explanation/description)

- a. ☐ Designed to military or intelligence standards or specifications.
- b. ☐ Designed for military application.
- c. ☐ Special characteristics (e.g. radiation-hardening, ballistic protection, hard points, TEMPEST capability, thermal or infrared signature reduction capability, surveillance or intelligence gathering capability).
- d. ☐ Commercial item modified for military application, provide nomenclature and model number to differentiate from commercial item.
- e. ☐ Commercial item modified for military application, state specific distinct difference between original commercial item and modified item.
- f. ☐ Services (provide comparable information as that which provided above and by marking this box, indicate it is for services versus hardware).

Explanation/Description (If the product is included in a higher assembly or end item, identify each higher assembly or end item that incorporates the product and its use. Identify all military applications and military capabilities of the product, and any equivalent products used for military application.) Summarize technical details of special characteristics (e.g. if image intensification tubes, provide level of technology, such as Gen II, Gen III, etc.). (limited to 600 characters)

N/A

D. Product Origin

9. Military/Commercial Modification of Commodity:

a. Was this commodity originally specifically designed or developed for a military use?

☐ Yes ☒ No

b. Was this commodity originally civil and subsequently adapted, configured or modified for a military use?

☐ Yes ☒ No

c. Was this commodity originally military and subsequently adapted, reconfigured or modified for commercial use?

☐ Yes ☒ No

d. Specifically define the modifications/changes and capabilities added to the commodity. List any differences in form, fit and/or function between the modified and unmodified versions: (limited to 600 characters)

N/A

☐ Supporting Documentation Attached

10. Status of Product Development: (Mark the status of the product and provide an explanation/description)

a. ☒ In Development

b. ☐ In Use

Explanation/Description (limited to 4000 characters)

To the best of Defense Distributed's knowledge, this file is conceptual in nature and has not been used to produce the insert.

☐ Supporting Documentation Attached

11. Funding History: (Check all that apply)

Include funding source contract or subcontract number and supporting documentation.

a. ☐ USG Agency

b. ☐ Foreign Government Agency

c. ☐ U.S. or Foreign Contractor

d. ☒ Self Funded

e. ☐ University Funded

Explanation/Description (limited to 600 characters)

To the best of Defense Distributed's knowledge, Pietro received no funding from any outside source for the creation of the file.

☐ Supporting Documentation Attached

12. U.S. and/or Foreign Availability of Identical Products: (Enter Foreign Export Controls, if known)

☒ None

Add Item

Remove Item

Manufacturer: _____

Commodity: _____

Model #: _____

In Use/In Development: _____

Foreign Exports Control: _____

Manufacturer's Website: _____

Explanation/Description (limited to 600 characters)

☐ Supporting Documentation Attached

E. Sales Information
13. Sales Information: (Select One) (See Block 13 Template)

Military and commercial sales data must be provided, as well as listing of the military and commercial customers. The information pertains specifically to the commodity/service in Block 8. Complete the attachment, if applicable. (Note: Submit one single file up to 35MB with sales information. Do not separate the sales information into multiple smaller files.)

☐ Sales Information Attachment (Template "Block 13 Sales Information") Attached

☒ No Sales

F. Miscellaneous Information
14. Has this Commodity been: (limited to 100 characters)

a. Has this Commodity been Previously Exported

☒ Yes ☐ No ☐ Unknown

If yes, cite U.S. Government licensing jurisdiction and provide license number, if applicable.

Posted to the internet as public domain information.

b. Has this Commodity been the subject of a Prior CJ?

☐ Yes ☐ No ☒ Unknown

If yes, Cite CJ Number.

(Applicant should list any prior CJ even if not submitted by them, e.g., submitted by Original Equipment Manufacturer (OEM), by the U.S. Government or by a third party.)

c. Has this Commodity been subject to a Department of Commerce Classification Request?

☐ Yes ☐ No ☒ Unknown

If yes, cite U.S. Government licensing jurisdiction and if under Department of Commerce, attach a copy with Export Control Classification Number (ECCN).

d. Has this Commodity been Exported under a Foreign Military Sale (FMS) case?

☐ Yes ☐ No ☒ Unknown

If yes, cite Foreign Military Sale (FMS) case number.

15. Description of the commodity and final DDTC action will be posted on the DDTC website for public access based on the information provided in Block 5 and any other descriptive information provided below. If you believe that any information contained in Block 5 is proprietary, please specifically identify the information below and provide summarized rationale for DDTC to consider withholding the information from public notice: (Limited to 600 characters. Additional justification may be provided as an attachment.)

N/A

16. Reason for Submitting CJ: (limited to 600 characters)

Per request of DTCC/END, Case No. 13-0001444.

17. Suggested U.S. Munitions List or Commerce Control List Number:

a. U.S. Munitions List (22 C.F.R. 121) Category/Sub Category

N/A

b. Export Administration Regulations (15 C.F.R. 730-774), Export Control Classification Number

N/A

18. Other Miscellaneous Information to be Considered that is not Otherwise Included in this Form: (e.g. U.S. Government Agency and point of contact information.) (limited to 300 characters)

☒ Supporting Documentation Attached

G. Applicant/Submitter's Certification

19. Applicant/Submitter's Certification: Note: ONLY this one page must be printed, signed, and scanned as an attachment.

Under Penalty According to Federal Law (See 22 CFR 127, 22 U.S.C. 2778, and 22 U.S.C. 1001).

I am the authorized employee of the company cited in Block 1, or a third party as described in Block 2 authorized to submit on behalf of the company in Block 4, and certify as to the accuracy and completeness of the information provided and have not knowingly omitted information that could have an impact on the final determination issued by the U.S. Department of State. Furthermore, I have specific authority to release for publication the text contained in Block 5.

Signature

Jahna M. Hartwig

Printed Name

06/21/2013

Date

☒ By checking this box, Applicant authorizes DITC to email the Commodity Jurisdiction determination as well as any other information associated with this case. The Commodity Jurisdiction determination will be mailed to the address below if box is not checked.

Name: Jahna M. Hartwig

Title: Partner

Company: Williams Mullen PC

Address: 1666 K St., NW, Suite 1200

City: Washington

State: DC

Zip Code: 20006

Phone #: 202-293-8145

Email: jhartwig@williamsmullen.com

Electronic Form Version Number: 1.2
For DDTC Use Only
CJ Number: _____

OMB APPROVAL NO: 1405-0163
EXPIRATION DATE: 01/31/2013
*ESTIMATED BURDEN: 10 Hours

U.S. Department of State

DS-4076 Commodity Jurisdiction (CJ) Determination Form

*PAPERWORK REDUCTION ACT STATEMENT: Public reporting burden for this collection of information is estimated to average 10 hours per response, including time required for searching existing data sources, gathering the necessary data, providing the information required, and reviewing the final collection. Send comments on the accuracy of this estimate of the burden and recommendations for reducing it to: Department of State (A/GIS/DIR) Washington, D.C. 20520.

A. Applicant Information

1. Applicant's Information: (Select all that apply)

Applicant is: ☐ Government ☐ Manufacturer ☐ Exporter ☐ Manufacturer's Representative ☒ Other

Applicant Name: (Company, Organization) Defense Distributed

Address: 711 W. 32nd Street, Apt. 115

City: Austin

State: TX

Zip Code: 78705

Phone #: 501-743-9680

PM/DDTC Registrant Code: _____

(If applicable)

Add Item

Remove Item

Name: (Point of Contact) Cody R. Wilson

Phone #: 501-743-9680

Fax #: _____

Email: crw@defdist.org

2. Submitter Information if other than Applicant in Block 1: (Complete if applicable)

Submitter Name: (Company, Organization) Williams Mullen PC

Address: 1666 K St., NW, Suite 1200

City: Washington

State: DC

Zip Code: 20006

Phone #: 202-293-8145

PM/DDTC Registrant Code: _____

(If applicable)

Add Item

Remove Item

Name: (Point of Contact) Jahna M. Hartwig

Phone #: 202-293-8145

Fax #: _____

Email: jhartwig@williamsmullen.com

☐ Attachment: Authorization from Applicant to Submitter authorizing submitter to file on its behalf and to release information in Block 5.

B. Transaction Description and Compliance Information

3. Transaction Description: (Note: No request involving Classified information will be considered.)

This Application Represents:

a. ☒ New Request

b. ☐ Resubmission

Prior CJ Case Number: _____

☐ Returned Without Action (RWA)

☐ Reconsideration (Include Prior CJ Determination Case Number)

Summarize Reason for Resubmission: (limited to 1200 characters)

Related to Compliance Matter: (limited to 1200 characters)

☒ Yes ☐ No

If yes, provide disclosure and/or case number (if available) and details to include U.S. Government Point of Contact. If status changes advise DDTC.

DTCC Case 13-0001444. This CJ is submitted at the request of DTCC/END in its letter to Defense Distributed dated May 8, 2013. The DTCC/END Compliance Specialist is assigned to this matter is Ms. Bridget Van Buren.

C. Commodity Description

4. Select Commodity Type: (Select all that apply) (22 C.F.R. 120.9, 120.10 and 121.8)

☐ End Item

☐ Component/Major

☐ Component/Minor

☐ Part

☐ Accessory/Attachment

☐ Software

☐ Firmware

☐ Services

☐ System

☒ Information or Technical Data

5. Commodity/Service Information: (Note: Complete all that apply and if not applicable, enter "N/A".)

a. Product Name: "The Dirty Diane" Oil Filter Silencer Adapter Data File

b. Model/Version Number: N/A

c. Part Number: N/A

d. National Stock Number: N/A

e. Other Identifier: (If applicable) N/A

f. Manufacturer: emptythemagazine

g. Service: N/A

h. Generic Description: SolidWorks CAD data file for an oil filter silencer adapter

i. Manufacturer's Website: <u>www.defdist.org</u> j. Commodity/Service Website: <u>http://defcad.com/the-dirty-diane-12-28-to-34-16-stp-s3600-oil-filter-silencer-adapter/</u> Note: Only one commodity may be entered; variants require separate submission. However, variants of a commodity or a family of commodities closely related, that is, major characteristics and descriptive information of the commodity are essentially the same and would be included in the same U.S. Munitions List category and subcategory may be considered.	
6. Additional Commodity Information/Documentation: (Brochures, Technical Information, Drawings, Schematics, Blue Prints, Course Syllabus/Handouts, Training Materials.) Attach product datasheet or other technical information such that an informed technical evaluation is possible.) Note: cost in U.S. Dollars. If unit is not listed in drop down list, e.g. service or training, enter the commodity. a. Cost Per Unit: <u>\$0.00</u> Copies <u> </u> b. Documentation Attached: <input checked="" type="checkbox"/> c. Patent Information: <u>n/a</u>	
7. Commodity/Service Description: (limited to 1200 characters) Brief summary of commodity or service (e.g. component used in aircraft communication system). Describe the product's use (what it does, how it operates, the components/system in which it is used and all current uses). Specify if commodity/service is controlled or restricted for public release by U.S. Government. <div style="border: 1px solid black; padding: 5px;"> The file is a Computer Aided Design (CAD) data file in the SolidWorks SLDPR file format for a model of an oil filter silencer adapter that is typically produced in stainless steel. If printed on a 3D printer, this item could be used as solvent trap adapter, which is used to catch solvents that are used in the process of cleaning a gun. While a metal solvent trap adapter could be used as a silencer, a plastic adapter would likely melt if used with a weapon as a silencer. </div>	
8. Identify any special and/or unique characteristics/capabilities: (Mark all boxes that apply and provide explanation/description) a. <input type="checkbox"/> Designed to military or intelligence standards or specifications. b. <input type="checkbox"/> Designed for military application. c. <input type="checkbox"/> Special characteristics (e.g. radiation-hardening, ballistic protection, hard points, TEMPEST capability, thermal or infrared signature reduction capability, surveillance or intelligence gathering capability). d. <input type="checkbox"/> Commercial item modified for military application, provide nomenclature and model number to differentiate from commercial item. e. <input type="checkbox"/> Commercial item modified for military application, state specific distinct difference between original commercial item and modified item. f. <input type="checkbox"/> Services (provide comparable information as that which provided above and by marking this box, indicate it is for services versus hardware). Explanation/Description (If the product is included in a higher assembly or end item, identify each higher assembly or end item that incorporates the product and its use. Identify all military applications and military capabilities of the product, and any equivalent products used for military application.) Summarize technical details of special characteristics (e.g. if image intensification tubes, provide level of technology, such as Gen II, Gen III, etc.). (limited to 600 characters) <u>N/A</u>	
D. Product Origin	
9. Military/Commercial Modification of Commodity: a. Was this commodity originally specifically designed or developed for a military use? <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No b. Was this commodity originally civil and subsequently adapted, configured or modified for a military use? <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No c. Was this commodity originally military and subsequently adapted, reconfigured or modified for commercial use? <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No d. Specifically define the modifications/changes and capabilities added to the commodity. List any differences in form, fit and/or function between the modified and unmodified versions: (limited to 600 characters) <u>N/A</u> <input type="checkbox"/> Supporting Documentation Attached	
10. Status of Product Development: (Mark the status of the product and provide an explanation/description) a. <input checked="" type="checkbox"/> In Development b. <input type="checkbox"/> In Use Explanation/Description (limited to 4000 characters) <div style="border: 1px solid black; padding: 5px;"> To the best of Defense Distributed's knowledge, this file is conceptual in nature and has not been used to produce a plastic oil filter silencer adapter. </div> <input type="checkbox"/> Supporting Documentation Attached	
11. Funding History: (Check all that apply) Include funding source contract or subcontract number and supporting documentation. a. <input type="checkbox"/> USG Agency b. <input type="checkbox"/> Foreign Government Agency c. <input type="checkbox"/> U.S. or Foreign Contractor d. <input checked="" type="checkbox"/> Self Funded e. <input type="checkbox"/> University Funded Explanation/Description (limited to 600 characters) <div style="border: 1px solid black; padding: 5px;"> To the best of Defense Distributed's knowledge, emptythemagazine received no funding from any outside source for the creation of the file. </div>	

<input type="checkbox"/> Supporting Documentation Attached	
12. U.S. and/or Foreign Availability of Identical Products: (Enter Foreign Export Controls, if known)	
<input type="checkbox"/> None Add Item	
<div style="background-color: #cccccc; padding: 2px;">Remove Item</div>	
Manufacturer: <u>Infinite Product Solutions</u>	
Commodity: <u>Stainless Solvent Trap 1/2-28 3/4-16 Thread Oil Filter Adapter</u>	
Model #: <u>N/A</u>	In Use/In Development: <u>In Use</u>
Foreign Exports Control: _____	
Manufacturer's Website: <u>http://www.infiniteproductsolutions.com/</u>	
<div style="background-color: #cccccc; padding: 2px;">Remove Item</div>	
Manufacturer: <u>Dead Iron Machining</u>	
Commodity: <u>1/2-28 ID X 3/4 - 16 Black Anodized Solvent Trap</u>	
Model #: <u>N/A</u>	In Use/In Development: <u>In Use</u>
Foreign Exports Control: _____	
Manufacturer's Website: <u>www.amazon.com/s/ref=bl_sr_automotive?_encoding=UTF8&field-brandtextbin=Dead%20Iron%20Machining&node</u>	
Explanation/Description (limited to 600 characters) (The items included in this section are examples of physical products available in stainless steel, rather than the identical CAD files. Solvent Trap Adapters are available from numerous manufacturers and available as commercial products on many websites, including amazon.com. (see http://www.amazon.com/s/ref=nb_sb_noss_1?url=search-alias%3Dautomotive&field-keywords=solvent+trap+adapter&rh=n%3A15684181%2Ck%3Asolvent+trap+adapter)	
<input checked="" type="checkbox"/> Supporting Documentation Attached	
E. Sales Information	
13. Sales Information: (Select One) (See Block 13 Template) Military and commercial sales data must be provided, as well as listing of the military and commercial customers. The information pertains specifically to the commodity/service in Block 8. Complete the attachment, if applicable. (Note: Submit one single file up to 35MB with sales information. Do not separate the sales information into multiple smaller files.)	
<input type="checkbox"/> Sales Information Attachment (Template "Block 13 Sales Information") Attached	
<input checked="" type="checkbox"/> No Sales	
F. Miscellaneous Information	
14. Has this Commodity been: (limited to 100 characters)	
a. Has this Commodity been Previously Exported <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Unknown If yes, cite U.S. Government licensing jurisdiction and provide license number, if applicable. <u>Posted to the internet as public domain information.</u>	
b. Has this Commodity been the subject of a Prior CJ? <input type="checkbox"/> Yes <input type="checkbox"/> No <input checked="" type="checkbox"/> Unknown If yes, Cite CJ Number. (Applicant should list any prior CJ even if not submitted by them, e.g., submitted by Original Equipment Manufacturer (OEM), by the U.S. Government or by a third party.) _____	
c. Has this Commodity been subject to a Department of Commerce Classification Request? <input type="checkbox"/> Yes <input type="checkbox"/> No <input checked="" type="checkbox"/> Unknown If yes, cite U.S. Government licensing jurisdiction and if under Department of Commerce, attach a copy with Export Control Classification Number (ECCN). _____	
d. Has this Commodity been Exported under a Foreign Military Sale (FMS) case? <input type="checkbox"/> Yes <input type="checkbox"/> No <input checked="" type="checkbox"/> Unknown If yes, cite Foreign Military Sale (FMS) case number. _____	
15. Description of the commodity and final DDTC action will be posted on the DDTC website for public access based on the information provided in Block 5 and any other descriptive information provided below. If you believe that any information contained in Block 5 is proprietary, please specifically identify the information below and provide summarized rationale for DDTC to consider withholding the information from public notice: (Limited to 600 characters. Additional justification may be provided as an attachment.) <u>N/A</u>	
16. Reason for Submitting CJ: (limited to 600 characters) <u>Per request of DTCC/END, Case No. 13-0001444.</u>	
17. Suggested U.S. Munitions List or Commerce Control List Number:	
a. U.S. Munitions List (22 C.F.R. 121) Category/Sub Category <u>N/A</u>	
b. Export Administration Regulations (15 C.F.R. 730-774), Export Control Classification Number <u>N/A</u>	

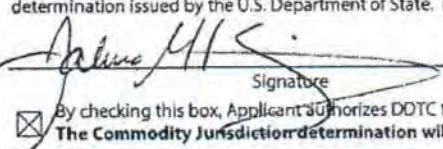
18. Other Miscellaneous Information to be Considered that is not Otherwise Included in this Form: (e.g. U.S. Government Agency and point of contact information.) (limited to 300 characters)
<div style="border: 1px solid black; height: 20px; width: 100%;"></div>
<input checked="" type="checkbox"/> Supporting Documentation Attached

G. Applicant/Submitter's Certification

19. Applicant/Submitter's Certification: Note: ONLY this one page must be printed, signed, and scanned as an attachment.

Under Penalty According to Federal Law (See 22 CFR 127, 22 U.S.C. 2778, and 22 U.S.C. 1001).

I am the authorized employee of the company cited in Block 1, or a third party as described in Block 2 authorized to submit on behalf of the company in Block 4, and certify as to the accuracy and completeness of the information provided and have not knowingly omitted information that could have an impact on the final determination issued by the U.S. Department of State. Furthermore, I have specific authority to release for publication the text contained in Block 5.

 Signature Jahna M. Hartwig Printed Name 06/21/2013 Date

☒ By checking this box, Applicant authorizes DDTC to email the Commodity Jurisdiction determination as well as any other information associated with this case. The Commodity Jurisdiction determination will be mailed to the address below if box is not checked.

Name: Jahna M. Hartwig
 Title: Partner
 Company: Williams Mullen PC
 Address: 1666 K St., NW, Suite 1200
 City: Washington State: DC Zip Code: 20006
 Phone #: 202-293-8145 Email: jhartwig@williamsmullen.com

Electronic Form Version Number: 1.2
For DDTC Use Only
CJ Number: _____

OMB APPROVAL NO. 1405-0163
EXPIRATION DATE: 01/31/2013
*ESTIMATED BURDEN: 10 Hours

U.S. Department of State

DS-4076 Commodity Jurisdiction (CJ) Determination Form

*PAPERWORK REDUCTION ACT STATEMENT: Public reporting burden for this collection of information is estimated to average 10 hours per response, including time required for searching existing data sources, gathering the necessary data, providing the information required, and reviewing the final collection. Send comments on the accuracy of this estimate of the burden and recommendations for reducing it to: Department of State (A/GIS/DIR) Washington, D.C. 20520.

A. Applicant Information

1. Applicant's Information: (Select all that apply)

Applicant is: ☐ Government ☐ Manufacturer ☐ Exporter ☐ Manufacturer's Representative ☒ Other

Applicant Name: (Company, Organization) Defense Distributed

Address: 711 W. 32nd Street, Apt. 115

City: Austin

State: TX

Zip Code: 78705

Phone #: 501-743-9680

PM/DDTC Registrant Code: _____

(If applicable)

Remove Item

Add Item

Name: (Point of Contact) Cody R. Wilson

Phone #: 501-743-9680

Fax #: _____

Email: crw@defdist.org

2. Submitter Information if other than Applicant in Block 1: (Complete if applicable)

Submitter Name: (Company, Organization) Williams Mullen PC

Address: 1666 K St., NW, Suite 1200

City: Washington

State: DC

Zip Code: 20006

Phone #: 202-293-8145

PM/DDTC Registrant Code: _____

(If applicable)

Remove Item

Add Item

Name: (Point of Contact) Jahna M. Hartwig

Phone #: 202-293-8145

Fax #: _____

Email: jhartwig@williamsmullen.com

☐ Attachment: Authorization from Applicant to Submitter authorizing submitter to file on its behalf and to release information in Block 5.

B. Transaction Description and Compliance Information

3. Transaction Description: (Note: No request involving Classified information will be considered.)

This Application Represents:

a. ☒ New Request

b. ☐ Resubmission

Prior CJ Case Number: _____

☐ Returned Without Action (RWA)

☐ Reconsideration (Include Prior CJ Determination Case Number)

Summarize Reason for Resubmission (limited to 1200 characters)

Related to Compliance Matter (limited to 1200 characters)

☒ Yes ☐ No

If yes, provide disclosure and/or case number (if available) and details to include U.S. Government Point of Contact. If status changes advise DDTC.

DTCC Case 13-0001444. This CJ is submitted at the request of DTCC/END in its letter to Defense Distributed dated May 8, 2013. The DTCC/END Compliance Specialist is assigned to this matter is Ms. Bridget Van Buren.

C. Commodity Description

4. Select Commodity Type: (Select all that apply) (22 C.F.R. 120.9, 120.10 and 121.8)

☐ End Item

☐ Component/Major

☐ Component/Minor

☐ Part

☐ Accessory/Attachment

☐ Software

☐ Firmware

☐ Services

☐ System

☒ Information or Technical Data

5. Commodity/Service Information: (Note: Complete all that apply and if not applicable, enter "N/A".)

a. Product Name: Voltlock Electronic Black Powder System Data Files

b. Model/Version Number: N/A

c. Part Number: N/A

d. National Stock Number: N/A

e. Other Identifier: (If applicable) N/A

f. Manufacturer: Mozi

g. Service: N/A

h. Generic Description: STL and IGS CAD files for models of cylinders of various bores with a touch hole

i. Manufacturer's Website:	www.defdist.org		
j. Commodity/Service Website:	http://defcad.com/voltlock-black-powder/		
Note: Only one commodity may be entered; variants require separate submission. However, variants of a commodity or a family of commodities closely related, that is, major characteristics and descriptive information of the commodity are essentially the same and would be included in the same U.S. Munitions List category and subcategory may be considered.			
6. Additional Commodity Information/Documentation:			
(Brochures, Technical Information, Drawings, Schematics, Blue Prints, Course Syllabus/Handouts, Training Materials.) Attach product datasheet or other technical information such that an informed technical evaluation is possible. Note: cost in U.S. Dollars. If unit is not listed in drop down list, e.g. service or training, enter the commodity.			
a. Cost Per Unit:	\$0.00	Copies	
b. Documentation Attached:	<input checked="" type="checkbox"/>		
c. Patent Information:	n/a		
7. Commodity/Service Description: (limited to 1200 characters)			
Brief summary of commodity or service (e.g. component used in aircraft communication system). Describe the product's use (what it does, how it operates, the components/system in which it is used and all current uses). Specify if commodity/service is controlled or restricted for public release by U.S. Government.			
The files are twelve CAD files for models of cylinders of various bores with a touch hole. Eleven of the files are in the STL file format and one is in the IGS format. If those pieces were printed on a 3D printer and used with an electronic ignition, the barrel would be expected to fail.			
8. Identify any special and/or unique characteristics/capabilities: (Mark all boxes that apply and provide explanation/description)			
a. <input type="checkbox"/> Designed to military or intelligence standards or specifications. b. <input type="checkbox"/> Designed for military application. c. <input type="checkbox"/> Special characteristics (e.g. radiation-hardening, ballistic protection, hard points, TEMPEST capability, thermal or infrared signature reduction capability, surveillance or intelligence gathering capability). d. <input type="checkbox"/> Commercial item modified for military application, provide nomenclature and model number to differentiate from commercial item. e. <input type="checkbox"/> Commercial item modified for military application, state specific distinct difference between original commercial item and modified item. f. <input type="checkbox"/> Services (provide comparable information as that which provided above and by marking this box, indicate it is for services versus hardware).			
Explanation/Description (If the product is included in a higher assembly or end item, identify each higher assembly or end item that incorporates the product and its use. Identify all military applications and military capabilities of the product, and any equivalent products used for military application.) Summarize technical details of special characteristics (e.g. if image intensification tubes, provide level of technology, such as Gen II, Gen III, etc.). (limited to 600 characters)			
N/A			
D. Product Origin			
9. Military/Commercial Modification of Commodity:			
a. Was this commodity originally specifically designed or developed for a military use? <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No			
b. Was this commodity originally civil and subsequently adapted, configured or modified for a military use? <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No			
c. Was this commodity originally military and subsequently adapted, reconfigured or modified for commercial use? <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No			
d. Specifically define the modifications/changes and capabilities added to the commodity. List any differences in form, fit and/or function between the modified and unmodified versions: (limited to 600 characters)			
N/A			
<input type="checkbox"/> Supporting Documentation Attached			
10. Status of Product Development: (Mark the status of the product and provide an explanation/description)			
a. <input checked="" type="checkbox"/> In Development b. <input type="checkbox"/> In Use			
Explanation/Description (limited to 4000 characters)			
To the best of Defense Distributed's knowledge, this file is conceptual in nature and has not been used to produce the plastic cylinders.			
<input type="checkbox"/> Supporting Documentation Attached			
11. Funding History: (Check all that apply)			
Include funding source contract or subcontract number and supporting documentation.			
a. <input type="checkbox"/> USG Agency b. <input type="checkbox"/> Foreign Government Agency c. <input type="checkbox"/> U.S. or Foreign Contractor d. <input checked="" type="checkbox"/> Self Funded e. <input type="checkbox"/> University Funded			
Explanation/Description (limited to 600 characters)			
To the best of Defense Distributed's knowledge, Mozi received no funding from any outside source for the creation of the file.			

☐ Supporting Documentation Attached

12. U.S. and/or Foreign Availability of Identical Products: (Enter Foreign Export Controls, if known)

☐ None

Add Item

Remove Item

Manufacturer: Allan Howard

Commodity: Ruger kmkiii6 stainless steel .22 automatic pistol with 6" barrel CAD Files

Model #: N/A

In Use/In Development: In Use

Foreign Exports Control:

Manufacturer's Website: <http://grabcad.com/library/ruger-kmkiii6-stainless-steel-22-automatic-pistol-with-6-barrel>

Remove Item

Manufacturer: Tom Prex

Commodity: .22lr pistol CAD files

Model #: N/A

In Use/In Development: In Use

Foreign Exports Control:

Manufacturer's Website: <http://grabcad.com/library/22lr-pistol>

Remove Item

Manufacturer: Fred Works

Commodity: Browning Buck Mark Threaded Barrel

Model #: N/A

In Use/In Development: In Use

Foreign Exports Control:

Manufacturer's Website: <http://grabcad.com/library/browning-buck-mark-threaded-barrel>

Explanation/Description (limited to 600 characters)

These CAD files are for a models of a complete .22 pistol, including the barrel and grip, as well as other components, and the barrel of a .22 caliber pistol.

☒ Supporting Documentation Attached

E. Sales Information
13. Sales Information: (Select One) (See Block 13 Template)

Military and commercial sales data must be provided, as well as listing of the military and commercial customers. The information pertains specifically to the commodity/service in Block 8. Complete the attachment, if applicable. (Note: Submit one single file up to 35MB with sales information. Do not separate the sales information into multiple smaller files.)

☐ Sales Information Attachment (Template "Block 13 Sales Information") Attached

☒ No Sales

F. Miscellaneous Information
14. Has this Commodity been: (limited to 100 characters)

a. Has this Commodity been Previously Exported

☒ Yes ☐ No ☐ Unknown

If yes, cite U.S. Government licensing jurisdiction and provide license number, if applicable.

Posted to the internet as public domain information.

b. Has this Commodity been the subject of a Prior CJ?

☐ Yes ☐ No ☒ Unknown

If yes, Cite CJ Number.

(Applicant should list any prior CJ even if not submitted by them, e.g., submitted by Original Equipment Manufacturer (OEM), by the U.S. Government or by a third party.)

c. Has this Commodity been subject to a Department of Commerce Classification Request?

☐ Yes ☐ No ☒ Unknown

If yes, cite U.S. Government licensing jurisdiction and if under Department of Commerce, attach a copy with Export Control Classification Number (ECCN).

d. Has this Commodity been Exported under a Foreign Military Sale (FMS) case?

☐ Yes ☐ No ☒ Unknown

If yes, cite Foreign Military Sale (FMS) case number.

15. Description of the commodity and final DDTC action will be posted on the DDTC website for public access based on the information provided in Block 5 and any other descriptive information provided below. If you believe that any information contained in Block 5 is proprietary, please specifically identify the information below and provide summarized rationale for DDTC to consider withholding the information from public notice: (Limited to 600 characters. Additional justification may be provided as an attachment.)

N/A

16. Reason for Submitting CJ: (limited to 600 characters)

Per request of DTCC/END, Case No. 13-0001444.

17. Suggested U.S. Munitions List or Commerce Control List Number:

a. U.S. Munitions List (22 C.F.R. 121) Category/Sub Category

N/A

b. Export Administration Regulations (15 C.F.R. 730-774), Export Control Classification Number

N/A

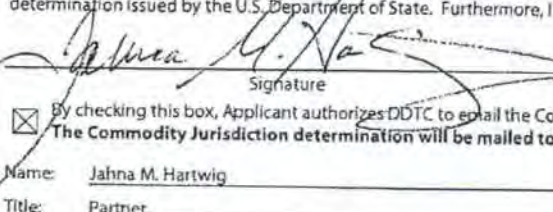
18. Other Miscellaneous Information to be Considered that is not Otherwise Included in this Form: (e.g. U.S. Government Agency and point of contact information.)
(limited to 300 characters)

☒ Supporting Documentation Attached

G. Applicant/Submitter's Certification

19. Applicant/Submitter's Certification: Note: ONLY this one page must be printed, signed, and scanned as an attachment.
Under Penalty According to Federal Law (See 22 CFR 127, 22 U.S.C. 2778, and 22 U.S.C. 1001).

I am the authorized employee of the company cited in Block 1, or a third party as described in Block 2 authorized to submit on behalf of the company in Block 4, and certify as to the accuracy and completeness of the information provided and have not knowingly omitted information that could have an impact on the final determination issued by the U.S. Department of State. Furthermore, I have specific authority to release for publication the text contained in Block 5.

 Signature _____ Jahna M. Hartwig Printed Name _____ 06/21/2013 Date _____

☒ By checking this box, Applicant authorizes DDTC to email the Commodity Jurisdiction determination as well as any other information associated with this case.
The Commodity Jurisdiction determination will be mailed to the address below if box is not checked.

Name: Jahna M. Hartwig

Title: Partner

Company: Williams Mullen PC

Address: 1666 K St., NW, Suite 1200

City: Washington State: DC Zip Code: 20006

Phone #: 202-293-8145 Email: jhartwig@williamsmullen.com

Electronic Form Version Number: 1.2
For DDTC Use Only
CJ Number: _____

OMB APPROVAL NO. 1405-0163
EXPIRATION DATE: 01/31/2013
*ESTIMATED BURDEN: 10 Hours

U.S. Department of State

DS-4076 Commodity Jurisdiction (CJ) Determination Form

*PAPERWORK REDUCTION ACT STATEMENT: Public reporting burden for this collection of information is estimated to average 10 hours per response, including time required for searching existing data sources, gathering the necessary data, providing the information required, and reviewing the final collection. Send comments on the accuracy of this estimate of the burden and recommendations for reducing it to: Department of State (A/GIS/DIR) Washington, D.C. 20520.

A. Applicant Information

1. Applicant's Information: (Select all that apply)

Applicant is: ☐ Government ☐ Manufacturer ☐ Exporter ☐ Manufacturer's Representative ☒ Other

Applicant Name: (Company, Organization) Defense Distributed

Address: 711 W. 32nd Street, Apt. 115

City: Austin

State: TX

Zip Code: 78705

Phone #: 501-743-9680

PM/DDTC Registrant Code: _____

(If applicable)

Add Item

Remove Item

Name: (Point of Contact) Cody R. Wilson

Phone #: 501-743-9680

Fax #: _____

Email: crw@defdist.org

2. Submitter Information if other than Applicant in Block 1: (Complete if applicable)

Submitter Name: (Company, Organization) Williams Mullen PC

Address: 1666 K St., NW, Suite 1200

City: Washington

State: DC

Zip Code: 20006

Phone #: 202-293-8145

PM/DDTC Registrant Code: _____

(If applicable)

Add Item

Remove Item

Name: (Point of Contact) Jahna M. Hartwig

Phone #: 202-293-8145

Fax #: _____

Email: jhartwig@williamsmullen.com

☐ Attachment: Authorization from Applicant to Submitter authorizing submitter to file on its behalf and to release information in Block 5.

B. Transaction Description and Compliance Information

3. Transaction Description: (Note: No request involving Classified information will be considered.) This Application Represents:

a. ☒ New Request

b. ☐ Resubmission

Prior CJ Case Number: _____

☐ Returned Without Action (RWA)

☐ Reconsideration (Include Prior CJ Determination Case Number)

Summarize Reason for Resubmission (limited to 1200 characters)

Related to Compliance Matter (limited to 1200 characters)

☒ Yes ☐ No

If yes, provide disclosure and/or case number (if available) and details to include U.S. Government Point of Contact. If status changes advise DDTC.

DTCC Case T3-0001444. This CJ is submitted at the request of DTCC/END in its letter to Defense Distributed dated May 8, 2013. The DTCC/END Compliance Specialist is assigned to this matter is Ms. Bridget Van Buren.

C. Commodity Description

4. Select Commodity Type: (Select all that apply) (22 C.F.R. 120.9, 120.10 and 121.8)

☐ End Item

☐ Component/Major

☐ Component/Minor

☐ Part

☐ Accessory/Attachment

☐ Software

☐ Firmware

☐ Services

☐ System

☒ Information or Technical Data

5. Commodity/Service Information: (Note: Complete all that apply and if not applicable, enter "N/A".)

a. Product Name: VZ-58 Front Sight Data Files

b. Model/Version Number: N/A

c. Part Number: N/A

d. National Stock Number: N/A

e. Other Identifier: (if applicable) N/A

f. Manufacturer: Reimo Soosaar

g. Service: N/A

h. Generic Description: Solidworks CAD file and rendering of a model of a site for a VZ-58 rifle.

i. Manufacturer's Website: <u>www.defdist.org</u> j. Commodity/Service Website: <u>http://defcad.com/vz-58-front-sight/</u> Note: Only one commodity may be entered; variants require separate submission. However, variants of a commodity or a family of commodities closely related, that is, major characteristics and descriptive information of the commodity are essentially the same and would be included in the same U.S. Munitions List category and subcategory may be considered.	
6. Additional Commodity Information/Documentation: (Brochures, Technical Information, Drawings, Schematics, Blue Prints, Course Syllabus/Handouts, Training Materials.) Attach product datasheet or other technical information such that an informed technical evaluation is possible. Note: cost in U.S. Dollars. If unit is not listed in drop down list, e.g. service or training, enter the commodity.	
a. Cost Per Unit: <u>\$0.00</u> Copies <u> </u> b. Documentation Attached: <input checked="" type="checkbox"/> c. Patent Information: <u>n/a</u>	
7. Commodity/Service Description: <i>(limited to 1200 characters)</i> Brief summary of commodity or service (e.g. component used in aircraft communication system). Describe the product's use (what it does, how it operates, the components/system in which it is used and all current uses). Specify if commodity/service is controlled or restricted for public release by U.S. Government. <div style="border: 1px solid black; padding: 2px;"> The files are a SolidWorks CAD file in the .SLDPRT file format and a rendering of a model of a sight for a VZ-58 rifle. If printed on a 3D printer and used with a weapon, the sight would be expected to fail. </div>	
8. Identify any special and/or unique characteristics/capabilities: (Mark all boxes that apply and provide explanation/description) a. <input type="checkbox"/> Designed to military or intelligence standards or specifications. b. <input type="checkbox"/> Designed for military application. c. <input type="checkbox"/> Special characteristics (e.g. radiation-hardening, ballistic protection, hard points, TEMPEST capability, thermal or infrared signature reduction capability, surveillance or intelligence gathering capability). d. <input type="checkbox"/> Commercial item modified for military application, provide nomenclature and model number to differentiate from commercial item. e. <input type="checkbox"/> Commercial item modified for military application, state specific distinct difference between original commercial item and modified item. f. <input type="checkbox"/> Services (provide comparable information as that which provided above and by marking this box, indicate it is for services versus hardware). Explanation/Description (If the product is included in a higher assembly or end item, identify each higher assembly or end item that incorporates the product and its use. Identify all military applications and military capabilities of the product, and any equivalent products used for military application.) Summarize technical details of special characteristics (e.g. if image intensification tubes, provide level of technology, such as Gen II, Gen III, etc.). <i>(limited to 600 characters)</i> <div style="border: 1px solid black; padding: 2px;"> N/A </div>	
D. Product Origin	
9. Military/Commercial Modification of Commodity: a. Was this commodity originally specifically designed or developed for a military use? <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No b. Was this commodity originally civil and subsequently adapted, configured or modified for a military use? <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No c. Was this commodity originally military and subsequently adapted, reconfigured or modified for commercial use? <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No d. Specifically define the modifications/changes and capabilities added to the commodity. List any differences in form, fit and/or function between the modified and unmodified versions: <i>(limited to 600 characters)</i> <div style="border: 1px solid black; padding: 2px;"> N/A </div> <input type="checkbox"/> Supporting Documentation Attached	
10. Status of Product Development: (Mark the status of the product and provide an explanation/description) a. <input checked="" type="checkbox"/> In Development b. <input type="checkbox"/> In Use Explanation/Description <i>(limited to 4000 characters)</i> <div style="border: 1px solid black; padding: 2px;"> To the best of Defense Distributed's knowledge, this file is conceptual in nature and has not been used to produce a plastic rifle sight model. </div> <input type="checkbox"/> Supporting Documentation Attached	
11. Funding History: (Check all that apply) Include funding source contract or subcontract number and supporting documentation. a. <input type="checkbox"/> USG Agency b. <input type="checkbox"/> Foreign Government Agency c. <input type="checkbox"/> U.S. or Foreign Contractor d. <input checked="" type="checkbox"/> Self Funded e. <input type="checkbox"/> University Funded Explanation/Description <i>(limited to 600 characters)</i> <div style="border: 1px solid black; padding: 2px;"> To the best of Defense Distributed's knowledge, Reimo Soosaar received no funding from any outside source for the creation of the file. </div>	

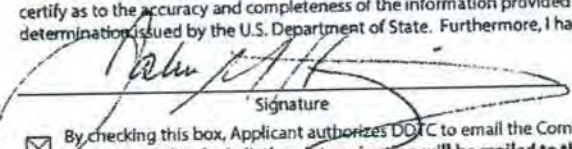
<input type="checkbox"/> Supporting Documentation Attached	
12. U.S. and/or Foreign Availability of Identical Products: (Enter Foreign Export Controls, if known)	
<input type="checkbox"/> None	<input type="button" value="Add Item"/>
<input type="button" value="Remove Item"/>	
Manufacturer: <u>Reimo Soosaar</u>	
Commodity: <u>Front sight for vz.58 rifle</u>	
Model #: <u>N/A</u>	In Use/In Development: <u>In Use</u>
Foreign Exports Control: _____	
Manufacturer's Website: <u>http://grabcad.com/library/front-sight-for-vz-dot-58-rifle</u>	
Explanation/Description (limited to 600 characters)	
<u>This file was published on Thingiverse in December 2012 and is still available on that site.</u>	
<input checked="" type="checkbox"/> Supporting Documentation Attached	
E. Sales Information	
13. Sales Information: (Select One) (See Block 13 Template)	
Military and commercial sales data must be provided, as well as listing of the military and commercial customers. The information pertains specifically to the commodity/service in Block 8. Complete the attachment, if applicable. (Note: Submit one single file up to 35MB with sales information. Do not separate the sales information into multiple smaller files.)	
<input type="checkbox"/> Sales Information Attachment (Template "Block 13 Sales Information") Attached	
<input checked="" type="checkbox"/> No Sales	
F. Miscellaneous Information	
14. Has this Commodity been: (limited to 100 characters)	
<div style="display: flex; justify-content: flex-end;"> <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Unknown </div>	
a. Has this Commodity been Previously Exported	
If yes, cite U.S. Government licensing jurisdiction and provide license number, if applicable.	
<u>Posted to the Internet as public domain information.</u>	
b. Has this Commodity been the subject of a Prior CJ?	
<div style="display: flex; justify-content: flex-end;"> <input type="checkbox"/> Yes <input type="checkbox"/> No <input checked="" type="checkbox"/> Unknown </div>	
If yes, Cite CJ Number.	
(Applicant should list any prior CJ even if not submitted by them, e.g., submitted by Original Equipment Manufacturer (OEM), by the U.S. Government or by a third party.)	
<u>_____</u>	
c. Has this Commodity been subject to a Department of Commerce Classification Request?	
<div style="display: flex; justify-content: flex-end;"> <input type="checkbox"/> Yes <input type="checkbox"/> No <input checked="" type="checkbox"/> Unknown </div>	
If yes, cite U.S. Government licensing jurisdiction and if under Department of Commerce, attach a copy with Export Control Classification Number (ECCN).	
<u>_____</u>	
d. Has this Commodity been Exported under a Foreign Military Sale (FMS) case?	
<div style="display: flex; justify-content: flex-end;"> <input type="checkbox"/> Yes <input type="checkbox"/> No <input checked="" type="checkbox"/> Unknown </div>	
If yes, cite Foreign Military Sale (FMS) case number.	
<u>_____</u>	
15. Description of the commodity and final DDTC action will be posted on the DDTC website for public access based on the information provided in Block 5 and any other descriptive information provided below. If you believe that any information contained in Block 5 is proprietary, please specifically identify the information below and provide summarized rationale for DDTC to consider withholding the information from public notice: (Limited to 600 characters. Additional justification may be provided as an attachment.)	
<u>N/A</u>	
16. Reason for Submitting CJ: (limited to 600 characters)	
<u>Per request of DTCC/END, Case No. 13-0001444.</u>	
17. Suggested U.S. Munitions List or Commerce Control List Number:	
a. U.S. Munitions List (22 C.F.R. 121) Category/Sub Category	
<u>N/A</u>	
b. Export Administration Regulations (15 C.F.R. 730-774), Export Control Classification Number	
<u>N/A</u>	
18. Other Miscellaneous Information to be Considered that is not Otherwise Included in this Form: (e.g. U.S. Government Agency and point of contact information.) (limited to 300 characters)	
<u>_____</u>	
<input checked="" type="checkbox"/> Supporting Documentation Attached	

10

G. Applicant/Submitter's Certification

19. Applicant/Submitter's Certification: Note: ONLY this one page must be printed, signed, and scanned as an attachment.
Under Penalty According to Federal Law (See 22 CFR 127, 22 U.S.C. 2778, and 22 U.S.C. 1001).

I am the authorized employee of the company cited in Block 1, or a third party as described in Block 2 authorized to submit on behalf of the company in Block 4, and certify as to the accuracy and completeness of the information provided and have not knowingly omitted information that could have an impact on the final determination issued by the U.S. Department of State. Furthermore, I have specific authority to release for publication the text contained in Block 5.

 Signature Jahna M. Hartwig Printed Name 06/21/2013 Date

☒ By checking this box, Applicant authorizes DDTC to email the Commodity Jurisdiction determination as well as any other information associated with this case.
The Commodity Jurisdiction determination will be mailed to the address below if box is not checked.

Name: Jahna M. Hartwig
Title: Partner
Company: Williams Mullen PC
Address: 1666 K St., NW, Suite 1200
City: Washington State: DC Zip Code: 20006
Phone #: 202-293-8145 Email: jhartwig@williamsmullen.com

Electronic Form Version Number: 1.2

For DDTC Use Only

CJ Number: _____

OMB APPROVAL NO. 1405-0163

EXPIRATION DATE: 01/31/2013

*ESTIMATED BURDEN: 10 Hours

U.S. Department of State

DS-4076 Commodity Jurisdiction (CJ) Determination Form

*PAPERWORK REDUCTION ACT STATEMENT: Public reporting burden for this collection of information is estimated to average 10 hours per response, including time required for searching existing data sources, gathering the necessary data, providing the information required, and reviewing the final collection. Send comments on the accuracy of this estimate of the burden and recommendations for reducing it to: Department of State (A/GIS/DIR) Washington, D.C. 20520.

A. Applicant Information**1. Applicant's Information: (Select all that apply)**Applicant is: ☐ Government ☐ Manufacturer ☐ Exporter ☐ Manufacturer's Representative ☒ OtherApplicant Name: (Company, Organization) Defense DistributedAddress: 711 W. 32nd Street, Apt. 115City: AustinState: TXZip Code: 78705Phone #: 501-743-9680

PM/DDTC Registrant Code: _____

(If applicable)

Add Item

Remove Item

Name: (Point of Contact) Cody R. WilsonPhone #: 501-743-9680

Fax #: _____

Email: crw@defdist.org**2. Submitter Information if other than Applicant in Block 1: (Complete if applicable)**Submitter Name: (Company, Organization) Williams Mullen PCAddress: 1666 K St., NW, Suite 1200City: WashingtonState: DCZip Code: 20006Phone #: 202-293-8145

PM/DDTC Registrant Code: _____

(If applicable)

Add Item

Remove Item

Name: (Point of Contact) Jahna M. HartwigPhone #: 202-293-8145

Fax #: _____

Email: jhartwig@williamsmullen.com☐ Attachment: Authorization from Applicant to Submitter authorizing submitter to file on its behalf and to release information in Block 5.**B. Transaction Description and Compliance Information****3. Transaction Description: (Note: No request involving Classified Information will be considered.)**

This Application Represents:

a. ☒ New Requestb. ☐ Resubmission

Prior CJ Case Number: _____

☐ Returned Without Action (RWA)☐ Reconsideration (Include Prior CJ Determination Case Number)

Summarize Reason for Resubmission (limited to 1200 characters)

Related to Compliance Matter (limited to 1200 characters)

☒ Yes ☐ No

If yes, provide disclosure and/or case number (if available) and details to include U.S. Government Point of Contact. If status changes advise DDTC.

DTCC Case 13-0001444. This CJ is submitted at the request of DTCC/END in its letter to Defense Distributed dated May 8, 2013. The DTCC/END Compliance Specialist is assigned to this matter is Ms. Bridget Van Buren.

C. Commodity Description**4. Select Commodity Type: (Select all that apply) (22 C.F.R. 120.9, 120.10 and 121.8)**☐ End Item☐ Component/Major☐ Component/Minor☐ Part☐ Accessory/Attachment☐ Software☐ Firmware☐ Services☐ System☒ Information or Technical Data**5. Commodity/Service Information: (Note: Complete all that apply and if not applicable, enter "N/A".)**a. Product Name: Springfield XD-40 Tactical Slide Assembly Data Filesb. Model/Version Number: N/Ac. Part Number: N/Ad. National Stock Number: N/Ae. Other Identifier: (If applicable) N/Af. Manufacturer: Gary Gg. Service: N/Ah. Generic Description: Nineteen SolidWorks CAD data files for components of a Springfield XD-40 Tactical Slide Assembly

i. Manufacturer's Website: <u>www.defdist.org</u>	j. Commodity/Service Website: <u>http://defcad.com/springfield-xd-40-tactical-slide-assembly/</u>
Note: Only one commodity may be entered; variants require separate submission. However, variants of a commodity or a family of commodities closely related, that is, major characteristics and descriptive information of the commodity are essentially the same and would be included in the same U.S. Munitions List category and subcategory may be considered.	
6. Additional Commodity Information/Documentation: (Brochures, Technical Information, Drawings, Schematics, Blue Prints, Course Syllabus/Handouts, Training Materials.) Attach product datasheet or other technical information such that an informed technical evaluation is possible.) Note: cost in U.S. Dollars. If unit is not listed in drop down list, e.g. service or training, enter the commodity.	
a. Cost Per Unit: <u>\$0.00</u>	Copies <u> </u>
b. Documentation Attached: <input checked="" type="checkbox"/>	
c. Patent Information: <u>n/a</u>	
7. Commodity/Service Description: (limited to 1200 characters) Brief summary of commodity or service (e.g. component used in aircraft communication system). Describe the product's use (what it does, how it operates, the components/system in which it is used and all current uses). Specify if commodity/service is controlled or restricted for public release by U.S. Government. <div style="border: 1px solid black; padding: 2px;"> The files are nineteen Computer Aided Design (CAD) data files in the SolidWorks .SLDPRT file format for models of components of a pistol slide for the Springfield XD-40. The components, if printed on a 3D printer, would be plastic pieces in the shape of the components of the slide assembly, but would be expected to fail if used with a weapon. </div>	
8. Identify any special and/or unique characteristics/capabilities: (Mark all boxes that apply and provide explanation/description)	
a. <input type="checkbox"/> Designed to military or intelligence standards or specifications. b. <input type="checkbox"/> Designed for military application. c. <input type="checkbox"/> Special characteristics (e.g. radiation-hardening, ballistic protection, hard points, TEMPEST capability, thermal or infrared signature reduction capability, surveillance or intelligence gathering capability). d. <input type="checkbox"/> Commercial item modified for military application, provide nomenclature and model number to differentiate from commercial item. e. <input type="checkbox"/> Commercial item modified for military application, state specific distinct difference between original commercial item and modified item. f. <input type="checkbox"/> Services (provide comparable information as that which provided above and by marking this box, indicate it is for services versus hardware). Explanation/Description (If the product is included in a higher assembly or end item, identify each higher assembly or end item that incorporates the product and its use. Identify all military applications and military capabilities of the product, and any equivalent products used for military application.) Summarize technical details of special characteristics (e.g. if image intensification tubes, provide level of technology, such as Gen II, Gen III, etc.). (limited to 600 characters) <div style="border: 1px solid black; padding: 2px;"> N/A </div>	
D. Product Origin	
9. Military/Commercial Modification of Commodity:	
a. Was this commodity originally specifically designed or developed for a military use? <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No	
b. Was this commodity originally civil and subsequently adapted, configured or modified for a military use? <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No	
c. Was this commodity originally military and subsequently adapted, reconfigured or modified for commercial use? <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No	
d. Specifically define the modifications/changes and capabilities added to the commodity. List any differences in form, fit and/or function between the modified and unmodified versions: (limited to 600 characters) <div style="border: 1px solid black; padding: 2px;"> N/A </div>	
<input type="checkbox"/> Supporting Documentation Attached	
10. Status of Product Development: (Mark the status of the product and provide an explanation/description)	
a. <input checked="" type="checkbox"/> In Development b. <input type="checkbox"/> In Use Explanation/Description (limited to 4000 characters) <div style="border: 1px solid black; padding: 2px;"> To the best of Defense Distributed's knowledge, this file is conceptual in nature and has not been used to produce the plastic model of the slide assembly. </div>	
<input type="checkbox"/> Supporting Documentation Attached	
11. Funding History: (Check all that apply) Include funding source contract or subcontract number and supporting documentation.	
a. <input type="checkbox"/> USG Agency b. <input type="checkbox"/> Foreign Government Agency c. <input type="checkbox"/> U.S. or Foreign Contractor d. <input checked="" type="checkbox"/> Self Funded e. <input type="checkbox"/> University Funded Explanation/Description (limited to 600 characters) <div style="border: 1px solid black; padding: 2px;"> To the best of Defense Distributed's knowledge, Gary G received no funding from any outside source for the creation of the file. </div>	

☐ Supporting Documentation Attached

12. U.S. and/or Foreign Availability of Identical Products: (Enter Foreign Export Controls, if known)

☐ None

Manufacturer: Reimo Soosaar

Commodity: Pistol Slide CAD files

Model #: N/A

In Use/In Development: In Use

Foreign Exports Control:

 Manufacturer's Website: <http://grabcad.com/library/pistol-slide-1>

Manufacturer: Dominic Megali

Commodity: Glock 21 slide

Model #: N/A

In Use/In Development: In Use

Foreign Exports Control:

 Manufacturer's Website: <http://grabcad.com/library/glock-21-slide>

Manufacturer: Steven Kiley

Commodity: Real sig p226 slide

Model #: N/A

In Use/In Development: In Use

Foreign Exports Control:

 Manufacturer's Website: <http://grabcad.com/library/real-sig-p226-slide>

Manufacturer: mutlu

Commodity: Colt m1911 slide assembly

Model #: N/A

In Use/In Development: In Use

Foreign Exports Control:

 Manufacturer's Website: <http://grabcad.com/library/colt-m1911-slide-assembly>

Explanation/Description (limited to 600 characters)

These CAD files contain drawings for models of various slide mechanisms.

☐ Supporting Documentation Attached

E. Sales Information
13. Sales Information: (Select One) (See Block 13 Template)

Military and commercial sales data must be provided, as well as listing of the military and commercial customers. The information pertains specifically to the commodity/service in Block 8. Complete the attachment, if applicable. (Note: Submit one single file up to 35MB with sales information. Do not separate the sales information into multiple smaller files.)

☐ Sales Information Attachment (Template "Block 13 Sales Information") Attached

☒ No Sales

F. Miscellaneous Information
14. Has this Commodity been: (limited to 100 characters)

a. Has this Commodity been Previously Exported

☒ Yes ☐ No ☐ Unknown

If yes, cite U.S. Government licensing jurisdiction and provide license number, if applicable.

Posted to the internet as public domain information.

b. Has this Commodity been the subject of a Prior CJ?

☐ Yes ☐ No ☒ Unknown

If yes, Cite CJ Number.

(Applicant should list any prior CJ even if not submitted by them, e.g., submitted by Original Equipment Manufacturer (OEM), by the U.S. Government or by a third party.)

c. Has this Commodity been subject to a Department of Commerce Classification Request?

☐ Yes ☐ No ☒ Unknown

If yes, cite U.S. Government licensing jurisdiction and if under Department of Commerce, attach a copy with Export Control Classification Number (ECCN).

d. Has this Commodity been Exported under a Foreign Military Sale (FMS) case?

☐ Yes ☐ No ☒ Unknown

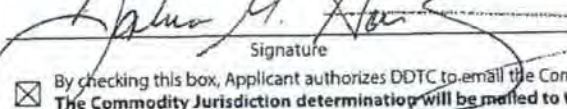
If yes, cite Foreign Military Sale (FMS) case number.

<p>15. Description of the commodity and final DDTC action will be posted on the DDTC website for public access based on the information provided in Block 5 and any other descriptive information provided below. If you believe that any information contained in Block 5 is proprietary, please specifically identify the information below and provide summarized rationale for DDTC to consider withholding the information from public notice: (Limited to 600 characters. Additional justification may be provided as an attachment.)</p> <p>N/A</p>	
<p>16. Reason for Submitting CJ: (limited to 600 characters)</p> <p>Per request of DTCC/END, Case No. 13-0001444.</p>	
<p>17. Suggested U.S. Munitions List or Commerce Control List Number:</p> <p>a. U.S. Munitions List (22 C.F.R. 121) Category/Sub Category</p> <p>N/A</p> <p>b. Export Administration Regulations (15 C.F.R. 730-774), Export Control Classification Number</p> <p>N/A</p>	
<p>18. Other Miscellaneous Information to be Considered that is not Otherwise Included in this Form: (e.g. U.S. Government Agency and point of contact information.) (limited to 300 characters)</p> <p></p> <p><input checked="" type="checkbox"/> Supporting Documentation Attached</p>	

G. Applicant/Submitter's Certification

19. Applicant/Submitter's Certification: Note: ONLY this one page must be printed, signed, and scanned as an attachment.
Under Penalty According to Federal Law (See 22 CFR 127, 22 U.S.C. 2778, and 22 U.S.C. 1001).

I am the authorized employee of the company cited in Block 1, or a third party as described in Block 2 authorized to submit on behalf of the company in Block 4, and certify as to the accuracy and completeness of the information provided and have not knowingly omitted information that could have an impact on the final determination issued by the U.S. Department of State. Furthermore, I have specific authority to release for publication the text contained in Block 5.

 Signature Jahna M. Hartwig Printed Name 06/21/2013 Date

☒ By checking this box, Applicant authorizes DDTC to email the Commodity Jurisdiction determination as well as any other information associated with this case.
The Commodity Jurisdiction determination will be mailed to the address below if box is not checked.

Name: Jahna M. Hartwig

Title: Partner

Company: Williams Mullen PC

Address: 1666 K St., NW, Suite 1200

City: Washington

State: DC

Zip Code: 20006

Phone #: 202-293-8145

Email: jhartwig@williamsmullen.com

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF TEXAS
AUSTIN DIVISION

DEFENSE DISTRIBUTED, et al.,	§	
Plaintiffs,	§	
	§	
v.	§	No. 1:15-cv-372-RP
	§	
U.S. DEPARTMENT OF STATE, et al.,	§	
Defendants.	§	

**DEFENDANTS' OPPOSITION TO PLAINTIFFS' MOTION FOR
A PRELIMINARY INJUNCTION**

TABLE OF CONTENTS

DEFENDANTS’ OPPOSITION TO PLAINTIFFS’ MOTION FOR A PRELIMINARY INJUNCTION	1
BACKGROUND	3
I. Statutory and Regulatory Framework.....	3
II. Defendants’ Regulation of Plaintiffs’ Conduct	4
LEGAL STANDARD	7
ARGUMENT.....	7
I. Plaintiffs’ Motion for a Preliminary Injunction Should Be Denied.	7
A. Plaintiffs Have Failed to Carry Their Burden of Demonstrating Irreparable Injury.	8
B. The Threatened Harm to the National Security and Foreign Policy Interests of the United States From an Injunction Outweighs any Irreparable Harm to Plaintiffs.	10
C. The Public Interest Would be Disserved By a Preliminary Injunction.	11
II. Plaintiffs’ Motion for a Preliminary Injunction Should Be Denied Because Plaintiffs Have Not Shown a Substantial Likelihood of Success on the Merits.....	11
A. The Export of CAD Files That Function to Automatically Create a Firearm or its Components is Not the Publishing of an Item of Expressive Speech.	11
B. Even If Limiting the Export of CAD Files Implicates the First Amendment, Defendants Are Likely to Prevail on Plaintiffs’ First Amendment Claims.	14
1. ITAR’s Export Controls Are a Valid, Content-Neutral Regulation of Plaintiffs’ Conduct That Do Not Infringe First Amendment Rights.	15
2. ITAR’s Export Controls Are Not a Facially Unconstitutional Prior Restraint.	18
3. ITAR’s Export Controls Are Not Unconstitutionally Overbroad.	21
B. Defendants Are Likely to Prevail on Plaintiffs’ Second Amendment Claims.	22
1. Plaintiffs Lack Standing for Their Second Amendment Claims.....	22
2. Plaintiffs Are Unlikely to Succeed on Their Second Amendment Claims.	25

C.	Defendants Are Likely to Prevail on Plaintiffs’ Other Claims.	27
1.	ITAR’s Standards Are Not Void for Vagueness.....	27
2.	Application of ITAR’s Export Requirements to Plaintiffs’ CAD Files Does Not Exceed the Statutory Authority Granted by Congress.....	28
CONCLUSION	31

TABLE OF AUTHORITIES

Cases

<i>AF Holdings, LLC. v. Does 1-1058</i> , 752 F.3d 990 (D.C. Cir. 2014)	6
<i>Alexander v. U.S.</i> , 509 U.S. 544 (1993)	18
<i>Bernstein v. U.S. Dep't of Justice</i> , 176 F.3d 1132 (9th Cir. 1999)	13
<i>Bonds v. Tandy</i> , 457 F.3d 409 (5th Cir. 2006)	24
<i>Broadrick v. Oklahoma</i> , 413 U.S. 601 (1973)	21
<i>Brockett v. Spokane Arcades</i> , 472 U.S. 491 (1985)	21, 22
<i>Brown v. District of Columbia</i> , 888 F. Supp. 2d 28 (D.D.C. 2012)	9
<i>Brown v. Entm't Merchants Ass'n</i> , 131 S. Ct. 2729 (2011)	12
<i>Brown v. Town of Cary</i> , 706 F.3d 294 (4th Cir. 2013)	28
<i>Bullfrog Films v. Wick</i> , 646 F. Supp. 492 (C.D. Cal. 1986)	14
<i>Canal Auth. of State of Fla. v. Callaway</i> , 489 F.2d 567 (5th Cir. 1974)	8
<i>Capital Cities/ABC, Inc. v. Brady</i> , 740 F. Supp. 1007 (S.D.N.Y. 1990)	16, 19
<i>Carey v. Population Servs. Int'l</i> , 431 U.S. 678 (1977)	25
<i>City of Lakewood v. Plain Dealer Pub. Co.</i> , 486 U.S. 750 (1988)	18, 19, 20, 21
<i>City of Littleton v. Z.J. Gifts D-4</i> , 541 U.S. 774 (2004)	20
<i>Clark v. Cmty. for Creative Non-Violence</i> , 468 U.S. 288 (1984)	15
<i>Coates v. City of Cincinnati</i> , 402 U.S. 611 (1971)	28
<i>Corrosion Proof Fittings v. EPA</i> , 947 F.2d 1201 (5th Cir. 1991),	25
<i>Ctr. for Biological Diversity v. Salazar</i> , 706 F.3d 1085 (9th Cir. 2013)	8
<i>DaimlerChrysler v. Cuno</i> , 547 U.S. 332 (2006)	23
<i>Dole v. Petroleum Treaters</i> , 876 F.2d 518 (5th Cir. 1989)	30
<i>Emergency Coal. to Defend Educ. Travel v. Dep't of Treas.</i> ,	

545 F.3d 4 (D.C. Cir. 2008)	16
<i>Escamilla v. M2,</i>	
Tech., 2013 WL 4577538 (E.D. Tex. 2013)	11
<i>Faculty Senate of Fla. Int'l U. v. Winn,</i>	
477 F. Supp. 2d 1198 (S.D. Fla. 2007)	9
<i>Feit v. Ward,</i>	
886 F.2d 848 (7th Cir. 1989)	1
<i>Forsyth Cnty., Ga. v. Nationalist Movement,</i>	
505 U.S. 123 (1992)	21
<i>Frank v. Relin,</i>	
1 F.3d 1317 (2d Cir. 1993)	1
<i>Freedman v. Maryland,</i>	
380 U.S. 51 (1965)	19, 20
<i>Gonannies, Inc. v. Goupair.Com, Inc.,</i>	
464 F. Supp. 2d 603 (N.D. Tex. 2006)	9
<i>Haig v. Agee,</i>	
453 U.S. 280 (1981)	14
<i>Heller v. District of Columbia,</i>	
670 F.3d 1244 (D.C. Cir. 2011)	27
<i>Henderson v. Stalder,</i>	
287 F.3d 374 (5th Cir. 2002)	23
<i>Holy Land Found. v. Ashcroft,</i>	
219 F. Supp. 2d 57 (D.D.C. 2002),	11
<i>House the Homeless v. Widnall,</i>	
94 F.3d 176 (5th Cir. 1996)	7, 12, 13
<i>Huitron-Guizar,</i>	
678 F.3d 1169	24
<i>Hurley v. Irish-Am. Gay, Lesbian & Bisexual Grp. of Boston,</i>	
515 U.S. 557 (1995)	12
<i>In re Iraq & Afg. Detainees Litig.,</i>	
479 F. Supp. 2d 85 (D.D.C. 2007)	2
<i>Johnson v. Moore,</i>	
958 F.2d 92 (5th Cir. 1992)	24
<i>Junger v. Daley,</i>	
209 F.3d 481 (6th Cir. 2000)	13
<i>Karn v. Dep't of State,</i>	
925 F.Supp. 1 (D.D.C.1996)	13
<i>Katt v. Dykhhouse,</i>	
983 F.2d 690 (6th Cir. 1992)	17
<i>Kirby v. City of Elizabeth,</i>	
388 F.3d 440 (4th Cir. 2004)	1
<i>Kleindienst v. Mandel,</i>	
408 U.S. 753 (1972)	18
<i>Kleinman v. City of San Marcos,</i>	
597 F.3d 323 (5th Cir. 2010)	17

<i>Laker Airways, Ltd. v. Pan Am. World Airways, Inc.</i> , 604 F. Supp. 280 (D.D.C. 1984).....	14
<i>Linick v. U.S.</i> , 104 Fed. Cl. 319 (Fed. Cl. 2012)	18
<i>Lorillard v. Pons</i> , 434 U.S. 575 (1978).....	30
<i>Lujan v. Defenders of Wildlife</i> , 504 U.S. 555 (1992).....	24
<i>Mance v. Holder</i> , 2015 WL 567302 (N.D. Tex. Feb. 11, 2015).....	25
<i>Marchese v. California</i> , 545 F.2d 645 (9th Cir. 1976)	26
<i>Martinez v. Mathews</i> , 544 F.2d 1233 (5th Cir. 1976)	passim
<i>Milena Ship Mgmt. Co. v. Newcomb</i> , 804 F. Supp. 846 (E.D. La. 1992).....	8
<i>Miss. State Democratic Party v. Barbour</i> , 529 F.3d 538 (5th Cir. 2008)	23
<i>Munn v. Ocean Springs, Miss.</i> , 763 F.3d 437 (5th Cir. 2014)	27, 28
<i>N.Y. State Club Ass'n v. City of New York</i> , 487 U.S. 1 (1987).....	21
<i>NAACP v. Kyle, Tex.</i> , 626 F.3d 233 (5th Cir. 2010)	23
<i>Nation Magazine v. Dep't of Def.</i> , 762 F. Supp. 1558 (S.D.N.Y. 1991).....	14
<i>Nat'l Rifle Ass'n v. ATF</i> , 700 F.3d 185 (5th Cir. 2012)	24, 25, 26, 27
<i>Near v. State of Minn.</i> , 283 U.S. 697 (1931).....	20
<i>Osterweil v. Edmonson</i> , 424 F. App'x 342 (5th Cir. 2011).....	24
<i>Planned Parenthood Ass'n of Hidalgo Cnty. Tex. v. Suehs</i> , 692 F.3d 343 (5th Cir. 2012)	2, 7, 14
<i>Promotions v. Conrad</i> , 420 U.S. 546 (1975).....	20
<i>Pub. Citizen, Inc. v. Bomer</i> , 274 F.3d 212 (5th Cir. 2001)	23
<i>Reeves v. McConn</i> , 631 F.2d 377 (5th Cir. 1980)	28
<i>Reliable Consultants, Inc. v. Earle</i> , 517 F.3d 738 (5th Cir. 2008)	25
<i>RTM Media, L.L.C. v. City of Houston</i> , 584 F.3d 220 (5th Cir. 2009)	17
<i>Scott v. Flowers</i> , 910 F.2d 201 (5th Cir. 1990)	1

<i>Sec'y State of Md. v. Munson</i> , 467 U.S. 947 (1984).....	22
<i>Siegel v. Lepore</i> , 234 F.3d 1163 (11th Cir. 2000)	9
<i>Spence v. Washington</i> , 418 U.S. 405 (1974).....	12
<i>Teague v. Reg'l Comm'r of Customs</i> , 404 F.2d 441 (2d Cir. 1968).....	20
<i>Texas v. Johnson</i> , 491 U.S. 397 (1989).....	12
<i>Thomas v. Chicago Park Dist.</i> , 534 U.S. 316 (2002).....	21
<i>Tough Traveler, Ltd. v. Outbound Prods.</i> , 60 F.3d 964 (2d Cir. 1995).....	9
<i>Turner Broad. Sys., Inc. v. FCC</i> , 512 U.S. 622 (1994).....	15
<i>U.S. Civil Service Comm. v. Nat'l Ass'n of Letter Carriers</i> , 413 U.S. 548 (1973).....	28
<i>U.S. v. 12 200-Ft. Reels</i> , 413 U.S. 123 (1972).....	14
<i>U.S. v. Bell</i> , 414 F.3d 474 (3d Cir. 2005).....	17
<i>U.S. v. Chi Mak</i> , 683 F.3d 1126 (9th Cir. 2012)	passim
<i>U.S. v. Edler Indus.</i> , 579 F.2d 516 (9th Cir. 1978)	passim
<i>U.S. v. Gurrola-Garcia</i> , 547 F.2d 1075 (9th Cir. 1976)	26
<i>U.S. v. Hicks</i> , 980 F.2d 963 (5th Cir. 1992)	21
<i>U.S. v. Hoffman</i> , 10 F.3d 808 (9th Cir. 1993)	17
<i>U.S. v. Huitron-Guizar</i> , 678 F.3d 1164 (10th Cir. 2012)	16
<i>U.S. v. Mandel</i> , 914 F.2d 1215 (9th Cir. 1990)	18
<i>U.S. v. Martinez</i> , 904 F.2d 601 (11th Cir. 1990)	18
<i>U.S. v. Marzzarella</i> , 614 F.3d 85 (3d Cir. 2010).....	26
<i>U.S. v. Merkt</i> , 794 F.2d 950 (5th Cir. 1986)	2
<i>U.S. v. O'Brien</i> , 391 U.S. 367 (1968).....	12, 17
<i>U.S. v. Posey</i> , 864 F.2d 1487 (9th Cir. 1989)	17, 18

<i>U.S. v. Ramsey</i> , 431 U.S. 606 (1977).....	2, 3
<i>U.S. v. South Carolina</i> , 720 F.3d 518 (4th Cir. 2013)	11
<i>U.S. v. W.T. Grant Co.</i> , 345 U.S. 629 (1953).....	9
<i>U.S. v. Yakou</i> , 428 F.3d 241 (D.C. Cir. 1995).....	30
<i>Voting for Am. v. Steen</i> , 732 F.3d 382 (5th Cir. 2013)	16
<i>W. Ala. Quality of Life Coal. v. U.S. Fed. Highway Admin.</i> , 302 F. Supp. 2d 672 (S.D. Tex. 2004)	9
<i>Ward v. Rock Against Racism</i> , 491 U.S. 781 (1989).....	15, 21
<i>Warth v. Seldin</i> , 422 U.S. 490 (1975).....	21
<i>Water Keeper Alliance v. Dep't of Def.</i> , 152 F. Supp. 2d 155 (D.P.R. 2001),.....	11
<i>Winter v. Natural Res. Def. Council</i> , 555 U.S. 7 (2008).....	7, 8, 11
<i>Wireless Agents, L.L.C. v. T-Mobile USA, Inc.</i> , No. 3:05-CV-0094, 2006 WL 1540587 (N.D. Tex. June 6, 2006)	9
<i>Wolfe v. Strankman</i> , 392 F.3d 358 (9th Cir. 2004)	1

Statutes

22 U.S.C. § 2751 et seq.,.....	3
22 U.S.C. § 2778(a)(1).....	3, 11, 15, 29
50 U.S.C. § 5(b) (1964)	20
22 U.S.C. § 2778(a)(2).....	29
22 U.S.C. § 2778(b)(1)(A)(i)	29
22 U.S.C. § 2778(b)(2)	29

Regulations

22 C.F.R. § 120.10	19, 21
22 C.F.R. § 120.10(a).....	28
22 C.F.R. § 120.10(a)(1)	7
22 C.F.R. § 120.10(a)(5).....	22
22 C.F.R. § 120.16	4
22 C.F.R. § 120.17(a)(1)	4
22 C.F.R. § 120.17(a)(3)	4
22 C.F.R. § 120.17(a)(4)	4
22 C.F.R. § 120.3	27
22 C.F.R. § 120.4	4
22 C.F.R. § 120.4(d)(1)-(2).....	5

22 C.F.R. § 121.1(I)(a).....	3
22 C.F.R. § 125.11	28
22 C.F.R. § 125.11(a)(1)	30
22 C.F.R. §§ 120-130.....	4
22 C.F.R. Part 120.....	16
22 C.F.R. Part 121.....	3, 19

Executive Orders

Executive Order 12637	4
-----------------------------	---

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF TEXAS
AUSTIN DIVISIONDEFENSE DISTRIBUTED, et al.,
Plaintiffs,

v.

U.S. DEPARTMENT OF STATE, et al.,
Defendants.§
§
§
§
§
§
§
§

No. 1:15-cv-372-RP

**DEFENDANTS' OPPOSITION TO PLAINTIFFS' MOTION FOR
A PRELIMINARY INJUNCTION**

At issue in this litigation is the United States' system of export controls for weapons—laws and regulations that seek to ensure that articles useful for warfare or terrorism are not shipped from the United States to other countries (or otherwise provided to foreigners), where, beyond the reach of U.S. law, they could be used to threaten U.S. national security, foreign policy, or international peace and stability. Plaintiffs challenge restrictions on the export of Computer Aided Design (“CAD”) files that are indispensable to the creation of guns and their components through a three-dimensional (“3D”) printing process. There is no dispute that the Government does not restrict Plaintiffs from sharing CAD files domestically or from using CAD files to make or acquire firearms in the United States. Nonetheless, Plaintiffs seek a mandatory preliminary injunction to bar the Government from preventing the *export* of these design files, which can be easily used to manufacture arms overseas. Plaintiffs' characterization of such an export as the mere “publication” of information is wrong—the CAD files unquestionably control the functioning of a 3D printer and cause it to manufacture firearms. Whatever informational value there may be in the process by which 3D printing occurs, the CAD files are also functional, directly facilitate the manufacture of weapons, and may properly be regulated for export. As set forth below, Plaintiffs' motion for a preliminary injunction should be denied.¹

¹ Injunctive relief designed to affect the conduct of a government entity is available only from official-capacity defendants. *See Scott v. Flowers*, 910 F.2d 201, 213 n.25 (5th Cir. 1990); *accord Wolfe v. Strankman*, 392 F.3d 358, 360 n.2 (9th Cir. 2004); *Kirby v. City of Elizabeth*, 388 F.3d 440, 452 n.10 (4th Cir. 2004); *Frank v. Relin*, 1 F.3d 1317, 1327 (2d Cir. 1993); *Feit v. Ward*, 886 F.2d 848, 858 (7th Cir. 1989); *In re Iraq & Afg. Detainees Litig.*, 479 F. Supp. 2d 85, 118-19 (D.D.C. 2007). This brief is therefore filed only on behalf of Defendants in their official

The Fifth Circuit and the Supreme Court have set forth a demanding four-part test to obtain a preliminary injunction and require that a party seeking such an “extraordinary remedy . . . clearly carr[y] the burden of persuasion” on each element. *Planned Parenthood Ass’n of Hidalgo Cnty. Tex. v. Suehs*, 692 F.3d 343, 348 (5th Cir. 2012). Plaintiffs here have not even attempted to demonstrate: (1) “a substantial threat of irreparable injury if the injunction were not granted,” (2) “that their substantial injury outweigh[s] the threatened harm to the party whom they [seek] to enjoin,” or (3) “that granting the preliminary injunction would not disserve the public interest.” *Id.* As Defendants show below, while Plaintiffs face little immediate harm, entry of an injunction would be likely to irrevocably harm national security and foreign policy and damage the public interest. Under these circumstances, Plaintiffs’ failure to address the legal requirements for a preliminary injunction alone warrants the straightforward denial of their motion without addressing the legal issues raised by Plaintiffs’ arguments on the merits.

Nonetheless, Plaintiffs also have no likelihood of success on the merits. The International Traffic in Arms Regulations (“ITAR”) regulate only the export of defense articles and defense services for the legitimate and important purpose of protecting national security and U.S. foreign policy interests. “Control of one’s borders . . . is an essential feature of national sovereignty,” *U.S. v. Merkt*, 794 F.2d 950, 955 (5th Cir. 1986), and it is well established that the United States has authority to regulate the trafficking of articles, particularly military articles, across those borders. *See U.S. v. Ramsey*, 431 U.S. 606, 619 (1977) (“border search” exception to Fourth Amendment rooted in “different rules of constitutional law” than apply domestically).

Plaintiffs characterize the cross-border transmission of digital instructions that automatically generate firearms as the “publication” of expression and claim that any licensing requirement on such export is an impermissible prior restraint on speech. But that claim is wrong both factually and legally. The Government does not seek to limit Plaintiffs from spreading ideas or information *about* 3D printing, but rather seeks to apply the generally applicable conduct regulation on exports of arms to CAD files that indisputably control the

capacities, and the term “Defendants,” as used herein, does not include the individual-capacity Defendants in this action.

functioning of a 3D printer and direct it to manufacture firearms. For these reasons, as other courts have concluded, the claim that the First Amendment forbids application of ITAR's export requirements to these items is meritless.

There is also no dispute that Plaintiffs may use these CAD files to make or acquire firearms in connection with their right to keep and bear arms under the Second Amendment. That Plaintiffs have not done so because they wish to "facilitat[e] *global* access to arms," Complaint ("Compl."), ECF No. 1 at ¶ 1,² calls into doubt whether their Second Amendment rights are even at issue, and in any case, Plaintiffs' Second Amendment and other claims likewise fail to satisfy the essential minimums of the legal theories that Plaintiffs assert. The Court should therefore deny Plaintiffs' motion.

BACKGROUND

I. Statutory and Regulatory Framework

The Arms Export Control Act ("AECA"), 22 U.S.C. § 2751 *et seq.*, authorizes the President, "[i]n furtherance of world peace and the security and foreign policy of the United States" to "control the import and the export of defense articles and defense services" and to promulgate regulations accordingly. 22 U.S.C. § 2778(a)(1). At the heart of the AECA is the United States Munitions List ("USML"), an extensive listing of materials that constitute "defense articles and defense services" under the AECA. 22 C.F.R. Part 121. Category I of the USML includes all firearms up to .50 caliber, and all technical data directly related to such firearms. *See* 22 C.F.R. § 121.1(I)(a). Technical data is information that "is required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance or modification of defense articles." *Id.* § 120.10(a).³ Section 2778(a) of the AECA authorizes the

² *See* Mem. in Support of Pls. Mot. for Prelim. Injunction, ECF No. 8 ("Pl. Br."), Ex. 1 ¶ 2 (Decl. of Cody Wilson); *id.* at App. 270 (deposit from prospective foreign "Ghost Gunner" buyer).

³ Technical data includes information in the form of blueprints, drawings, photographs, plans, instructions or documentation," and broadly exempts information already in the public domain, as defined in Section 120.11. *Id.* § 120.10. On June 3, 2014, the State Department issued a Notice of Proposed Rulemaking to update, *inter alia*, the definitions of "technical data" in the ITAR, the scope of the "public domain" exemption, and the application of ITAR to technical data on the Internet. *See* 80 Fed. Reg. 31525; Aguirre Decl. ¶ 11. The proposal would clarify that CAD files are a form of "technical data" and make explicit that providing technical data on a publicly accessible network, such as the Internet, is an export because of its inherent accessibility to foreign powers. 80 Fed. Reg. 31525. As relevant here, the clarified definitions in this NPRM

President: (1) to designate those defense articles and services to be included on the USML; (2) to require licenses for the export of items on the USML; and (3) to promulgate regulations for the import and export of such items on the USML. *Id.* The President has delegated to the State Department this authority, and the Department has accordingly promulgated the ITAR, which is administered by the State Department's Directorate of Defense Trade Controls ("DDTC"). *See* Executive Order 13637(n)(iii); 22 C.F.R. §§ 120-130.

Importantly, ITAR does not regulate any activities except those that constitute "exports," *i.e.*, the transfer of defense articles abroad or to foreign persons. ITAR's definition of exports includes, in relevant part: (1) "[s]ending or taking a defense article out of the United States in any manner," 22 C.F.R. § 120.17(a)(1); (2) "[d]isclosing (including oral or visual disclosure) or transferring in the United States any defense article to an embassy, any agency or subdivision of a foreign government," *id.* § 120.17(a)(3); and (3) "[d]isclosing (including oral or visual disclosure) or transferring technical data to a foreign person, whether in the United States or abroad." *Id.* § 120.17(a)(4).

In the vast majority of circumstances, there is no doubt as to whether a particular item to be exported is a defense article or defense service. *See* Declaration of Lisa V. Aguirre ("Aguirre Decl.") ¶ 19. For those cases in which there is doubt, however, ITAR contains a "commodity jurisdiction" ("CJ") procedure. Upon written request, the DDTC will provide potential exporters with a determination as to whether the item, service, or data is within the scope of ITAR. 22 C.F.R. § 120.4. These assessments are made on a case-by-case basis through an inter-agency process, evaluating whether the article is covered by the USML, is functionally equivalent to an article on the USML, or has substantial military or intelligence application. *See id.* § 120.4(d).

II. Defendants' Regulation of Plaintiffs' Conduct

On May 8, 2013, shortly after learning about Defense Distributed's unrestricted posting of CAD files to the Internet, the DDTC's Enforcement Division sent a letter to Defense Distributed noting that "it is unlawful to export any defense article or technical data for which a

would simply confirm that treatment of the Plaintiffs' posting of the CAD files to the Internet under the current regulations would remain the same, and thus Defendants do not anticipate the NPRM would impact application of the ITAR to the files at issue in this case.

license or written approval is required without first obtaining the required authorization from the DDTC.” Pl. Br. at App. 14; *see* Ex. 1. Observing that “disclosing (including oral or visual disclosure) or transferring foreign data to a foreign person, whether in the United States or abroad, is considered an export,” DDTC requested that Defense Distributed submit CJ determination requests for ten CAD files and that Defense Distributed “treat [this] technical data as ITAR-controlled” until DDTC could “provide[] Defense Distributed with final CJ determinations.” Pl. Br. at App. 14-15. These files included “a trigger guard, grips, two receivers, a magazine for AR-15 rifles, and a handgun named ‘The Liberator.’” Pl. Br. at App. 1, ¶ 3. DDTC therefore suggested that the technical data be removed from Defense Distributed’s website—*i.e.*, a location in which it would be disclosed without limitation to a foreign person, *see* 22 C.F.R. § 120.16, should any foreign person visit Defense Distributed’s website and download the file, during the review process. Defendants did not suggest in any way that Defense Distributed’s CAD files could not be provided to U.S. persons within the U.S. or otherwise used, altered, or discussed in ways that would not constitute “exports.”

On June 21, 2013, Defense Distributed filed CJ requests for the ten items identified in the DDTC letter. Defense Distributed described its submissions as “data files” that are “essentially blueprints that can be read by CAD software . . . [as] a means of creating physical 3D models of objects.” Pl. Br. at App. 208. These data files instruct 3D printers to create:

- (1) sixteen . . . parts and components of the [“Liberator”] pistol [which] could be assembled into a single shot .380 caliber firearm;
- (2) a barrel and grip for a .22 caliber pistol;
- (3) a solid piece of plastic in the shape of [a 125 mm BK-14M High Explosive Anti-Tank (“HEAT”) Warhead];
- (4) a plastic piece in the shape of [a 5.56/.223] muzzle brake;
- (5) nineteen . . . components of a pistol slide for the Springfield XD-40;
- (6) a slip-on sound moderator for an air gun;
- (7) “The Dirty Diane” . . . an oil filter silencer adapter;
- (8) a model of a sub-caliber insert [for] a cylinder with a .22 bore;
- (9) Voltock Electronic Black Powder System . . . models of cylinders of various bores;
- (10) a model of a sight for a VZ-58 rifle.

Pl. Br. at App. 210.

At no time did Defense Distributed inquire about whether ITAR would affect its distribution of CAD files to U.S. persons within the United States or would limit its ability, or

that of other U.S. persons, to use the CAD files in 3D printing.⁴

While the Government reviewed Defense Distributed's first CJ ten requests, Defense Distributed submitted an additional request on January 2, 2015, seeking a determination on: (1) the "Ghost Gunner," a "3-axis, computer-numerically-controlled [machine] . . . designed, developed, and manufactured by Defense Distributed to *automatically manufacture* publicly available designs with nearly zero user interaction." Pl. Br. at App. 267 (emphasis added). On April 15, 2015, DDTC provided a CJ determination to Defense Distributed, finding that the Ghost Gunner would not be subject to the jurisdiction of the Department of State (although "project files, data files, or any form of technical data for producing a defense article" would be subject to ITAR jurisdiction). *Id.* at App. 280-81.

On June 4, 2015, review of Defense Distributed's first ten requests was completed and DDTC provided CJ determinations for the requested items. *See* Aguirre Decl. ¶ 28. As explained in DDTC's determination letter, the Department of State determined that only six of the CAD files were subject to ITAR control: those for the "Liberator pistol," ".22 [caliber] electric [pistol]," "5.56/.223 muzzle brake," "Springfield XD-40 tactical slide assemble," "sub-caliber insert," and "VZ-58 front sight." *Id.* In finding the CAD files to be within the commodity jurisdiction of the State Department, DDTC classified the CAD files as technical data under Category I, subsection (i) of the USML, relying on the definition of technical data in § 120.10(a)(1). As DDTC's letter explained, these determinations require that a "license or other approval . . . pursuant to the ITAR" be obtained before any export of these CAD files. *Id.*

As to the items determined to be within ITAR's commodity jurisdiction, the CJ review process concluded that Defense Distributed's CAD files constitute electronic data that can be used, in conjunction with a 3D printer, to automatically, and without further human intervention, generate a defense article or a component of a defense article identified on the USML. *See*

⁴ ITAR jurisdiction is limited to *exports* of defense articles and related technical data and does not prohibit the transmission of defense articles from one U.S. person to another known to be a U.S. person within the U.S. Although DDTC's May 8, 2013 letter expressed DDTC's concerns about Defense Distributed's unrestricted postings to the Internet, the availability of online material to users outside the U.S. can be limited in a number of ways. For example, Internet users can be generally located using their Internet Protocol addresses. *See generally AF Holdings, v. Does 1-1058*, 752 F.3d 990, 996 (D.C. Cir. 2014) (discussing geolocation services).

Aguirre Decl. ¶¶ 29-30. The CAD files are “technical data” that are regulated by the ITAR because, absent such regulation, providing the CAD designs to a foreign person or foreign government would be equivalent to providing the defense article itself, enabling the complete circumvention of ITAR’s export regulations.

LEGAL STANDARD

“A preliminary injunction is an extraordinary remedy never awarded as of right.” *Winter v. Natural Res. Def. Council*, 555 U.S. 7, 24 (2008). Rather, a plaintiff seeking a preliminary injunction must show: “(1) a substantial likelihood of success on the merits, (2) a substantial threat of irreparable injury if the injunction were not granted, (3) that their substantial injury outweighed the threatened harm to the party whom they sought to enjoin, and (4) that granting the preliminary injunction would not disserve the public interest.” *Suehs*, 692 F.3d at 348. “In each case, courts must balance the competing claims of injury and must consider the effect on each party of the granting or withholding of the requested relief.” *Winter*, 555 U.S. at 24. Due to its “extraordinary” nature, no preliminary injunction should be “granted unless the party seeking it has clearly carried the burden of persuasion on all four requirements.” *Id.* (internal quotation omitted).

Here, Plaintiffs’ burden is even higher, given the nature of the injunction they seek. Plaintiffs ask this Court to enjoin Defendants “from enforcing any prepublication approval requirement against unclassified information under the International Traffic in Arms Regulations.” Proposed Order, ECF No. 7, at 1. This request constitutes “[m]andatory preliminary relief, which goes well beyond simply maintaining the status quo *pendente lite*.” *Martinez v. Mathews*, 544 F.2d 1233, 1243 (5th Cir. 1976) (citations omitted). Such relief “is particularly disfavored, and should not be issued unless the facts and law clearly favor the moving party.” *Id.* (citations omitted); *see also Milena Ship Mgmt. Co. v. Newcomb*, 804 F. Supp. 846, 852-55 (E.D. La. 1992).

ARGUMENT

I. Plaintiffs’ Motion for a Preliminary Injunction Should Be Denied.

Plaintiffs must persuasively demonstrate that each of the four conditions for a preliminary

injunction is met, not just a single element of their choosing. *See Winter*, 555 U.S. at 20. This requirement serves interests of critical importance; among them, “preserv[ation] of the court’s ability to render a meaningful decision on the merits” based on a fully developed record and the reasoned and considered arguments of the parties. *Canal Auth. of State of Fla. v. Callaway*, 489 F.2d 567, 573 (5th Cir. 1974); *Ctr. for Biological Diversity v. Salazar*, 706 F.3d 1085, 1090 (9th Cir. 2013). Nevertheless, Plaintiffs have elected to rely on only one element of the standard: their likelihood of success. They give short shrift—less than one page in a brief for which the Court granted leave to extend the page limits to thirty—to the three other elements. Plaintiffs’ failure to address these other elements alone warrants denial of their motion.

A. Plaintiffs Have Failed to Carry Their Burden of Demonstrating Irreparable Injury.

As the Supreme Court explained in *Winter*, because “[a] preliminary injunction is an extraordinary remedy,” courts must consider the actual “effect on each party of the granting or withholding” of relief and do so “[i]n each case.” 555 U.S. at 24. But Plaintiffs have disregarded this principle and offered no specifics to support their claim of irreparable harm other than the allegation that Defendants have infringed upon their constitutional rights. *See* Pl. Br. at 29. This *pro forma* statement—particularly in light of Defendants’ demonstration below that Plaintiffs’ rights have not been violated—is insufficient to carry Plaintiffs’ burden to obtain a mandatory injunction.

The presumption that alleged violations of constitutional rights can be sufficient to presume irreparable injury for purposes of injunctive relief should only be made “where there is an ‘imminent likelihood that *pure speech* will be chilled or prevented altogether’,” and the circumstances presented here undercut Plaintiffs’ argument that such injury has occurred. *Faculty Senate of Fla. Int’l U. v. Winn*, 477 F. Supp. 2d 1198 (S.D. Fla. 2007) (declining to find irreparable harm in limits on foreign academic research) (quoting *Siegel v. Lepore*, 234 F.3d 1163, 1178 (11th Cir. 2000) (en banc)). First, Plaintiffs’ claim of imminent irreparable injury is significantly undermined by their delay in seeking judicial relief. Plaintiffs challenge the State Department’s application of the ITAR to unrestricted postings of technical data on their website—an application of which they have been aware since receiving the State Department’s

May 8, 2013 letter. *See* Compl. ¶¶ 25-27. Nearly two years later, on May 6, 2015, Plaintiffs filed this lawsuit. ECF No. 1. “[D]elay in seeking a remedy is an important factor bearing on the need for a preliminary injunction.” *Gonannies, Inc. v. Goupair.Com, Inc.*, 464 F. Supp. 2d 603, 609 (N.D. Tex. 2006) (quoting *Wireless Agents, L.L.C. v. T-Mobile USA, Inc.*, No. 3:05-CV-0094, 2006 WL 1540587, at *3 (N.D. Tex. June 6, 2006)). The two-year delay between the challenged action and the filing of this lawsuit seriously “undercuts the sense of urgency that ordinarily accompanies a motion for preliminary relief and suggests that there is, in fact, no irreparable injury.” *Tough Traveler, Ltd. v. Outbound Prods.*, 60 F.3d 964, 968 (2d Cir. 1995) (internal quotation marks and citation omitted); *see Brown v. District of Columbia*, 888 F. Supp. 2d 28, 32 (D.D.C. 2012) (noting as relevant to the irreparable harm analysis the fact that plaintiff waited almost seven months to file lawsuit).

Second, irreparable harm can be “neither speculative nor remote,” but must be “actual and imminent.” *W. Ala. Quality of Life Coal. v. U.S. Fed. Highway Admin.*, 302 F. Supp. 2d 672, 684 (S.D. Tex. 2004) (quoting *U.S. v. W.T. Grant Co.*, 345 U.S. 629, 633 (1953)). As discussed above, the State Department’s jurisdiction over Defense Distributed’s technical data extends only to its export, and the State Department has not suggested that ITAR imposes any limitation on Plaintiffs’ actual distribution of technical data to U.S. persons in the United States. Yet despite actual knowledge of U.S. persons interested in obtaining this technical data, allegedly including co-Plaintiff Second Amendment Foundation (“SAF”) and some of its members, Defense Distributed has apparently done nothing to distribute the technical data in a manner that would not constitute an export. Nor have Plaintiffs made any inquiry of Defendants about any measures Defense Distributed could take that would allow it to post the technical data on the Internet without violating ITAR. Plaintiffs’ apparent failure to exercise these options undermines their claim that they have incurred an actual, imminent, and irreparable harm. In these circumstances, Plaintiffs’ brief citation to inapposite case law does not demonstrate “irreparable injury,” let alone satisfy the heightened standard for a mandatory injunction.⁵

⁵ The cases relied on by Plaintiffs presented immediate instances of harm not illustrated in Plaintiffs’ threadbare allegations here. For example, in *Deerfield Med. Ctr. v. Deerfield Beach*, irreparable harm existed with respect to an abortion clinic denied zoning privileges and its

B. The Threatened Harm to the National Security and Foreign Policy Interests of the United States From an Injunction Outweighs any Irreparable Harm to Plaintiffs.

As explained in detail in the Declaration of Lisa V. Aguirre, Director of the Office of Defense Trade Controls Management, the Department of State has concluded that: (1) export of Defense Distributed's CAD files could cause serious harm to U.S. national security and foreign policy interests; and (2) a preliminary injunction in this case would be likely to cause such harm.

As Plaintiffs described in their submissions to Defendants, their CAD files constitute the functional equivalent of defense articles: capable, in the hands of anyone who possesses commercially available 3D printing equipment, of "automatically" generating a lethal firearm that can be easily modified to be virtually undetectable in metal detectors and other security equipment. *See* Aguirre Decl. ¶ 35; Pl. Br. at App. 208-59.⁶ The unrestricted provision of such undetectable firearms by U.S. persons to individuals in other countries—particularly those countries with stricter firearms regulations that may not have the same security preparedness as the United States—presents a serious risk of acts of violence in those countries. The State Department is particularly concerned that Plaintiffs' proposed export of undetectable firearms technology could be used in an assassination, for the manufacture of spare parts by embargoed nations, terrorist groups, or guerrilla groups, or to compromise aviation security overseas in a manner specifically directed at U.S. persons.⁷ *See* Aguirre Decl. ¶ 35. As with the export of firearms themselves, these potential risks to U.S. foreign policy and national security interests warrant subjecting Defense Distributed's CAD files to ITAR's export licensing of technical data.

C. The Public Interest Would be Disserved By a Preliminary Injunction.

The threat of harm to U.S. foreign policy and national security interests tilts the public

"physician and those women for whom he would otherwise perform the operation in the meantime." 661 F.2d 328, 338 (5th Cir. 1981). Similarly, in *Elrod v. Burns*, the Court found irreparable injury where challenged patronage requirements imposed on plaintiffs an obligation to "pledge [] allegiance to another political party" and avoid "associat[ing] with others of [their] political persuasion." 427 U.S. 347, 355-56 (1976).

⁶ Indeed, in part for this reason, the Liberator design includes the insertion a sufficient amount of metal into the resulting firearm to ensure its detectability. *See* Aguirre Decl. ¶ 35. Although this instruction promotes users' compliance with federal law prohibiting the manufacture of undetectable firearms, federal law does not prevent the manufacture of undetectable firearms by users outside the United States, and the Liberator remains operable without the inserted metal.

⁷ The harm is reinforced by the fact that entry of an injunction is likely to bring attention to the availability of the CAD files on the Internet. *See* Aguirre Decl. ¶ 37.

interest factor heavily in the Government's favor, particularly in the context of a mandatory injunction. *See Winter*, 555 U.S. at 24; *U.S. v. South Carolina*, 720 F.3d 518, 533 (4th Cir. 2013) ("injury to the nation's foreign policy" weighs in favor of the United States in public interest inquiry); *accord Water Keeper Alliance v. Dep't of Def.*, 152 F. Supp. 2d 155, 163 (D.P.R. 2001), *aff'd* 271 F.3d 21, 34-35 (1st Cir. 2001). This is true even where, as here, the harms from an injunction are likely to be felt abroad rather than domestically, because—as recognized by Congress in enacting the AECA, *see* 22 U.S.C. § 2778(a)(1)—"[b]oth the Government and the public have a strong interest in curbing" violent regional conflicts elsewhere in the world, especially when such conflict implicates "the security of the United States and the world as a whole." *Holy Land Found. v. Ashcroft*, 219 F. Supp. 2d 57, 84 (D.D.C. 2002), *aff'd* 333 F.3d 156 (D.C. Cir. 2003). Plaintiffs' barebones discussion of the public interest cannot supersede the demonstrated possibility of harm to national security and foreign policy provided by Defendants. *See Escamilla v. M2 Tech.*, 2013 WL 4577538 (E.D. Tex. 2013) (injunction that would harm "issues of national security," even "indirectly," would disserve public interest).⁸

II. Plaintiffs' Motion for a Preliminary Injunction Should Be Denied Because Plaintiffs Have Not Shown a Substantial Likelihood of Success on the Merits.

Plaintiffs have also failed to demonstrate either a likelihood of success on the merits for a preliminary injunction or that "the facts and law clearly favor" their claims; accordingly, they have failed to meet their burden for a mandatory injunction. *See Martinez*, 544 F.2d at 1243.

A. The Export of CAD Files That Function to Automatically Create a Firearm or its Components is Not the Publishing of an Item of Expressive Speech.

Underpinning Plaintiffs' First Amendment claims is the assumption that Plaintiffs seek to "publish" CAD files for 3D printers and that doing so is no different than the "publication of an idea." Pl. Br. at 14-15. Plaintiffs themselves recognize this is a critical threshold issue on which they must succeed, *see id.*, but they have failed to make the requisite showing on the merits to obtain a mandatory preliminary injunction.

⁸ Importantly, because ITAR restricts only exports, any public interest in persons in the U.S. obtaining Defense Distributed's CAD files, whether to manufacture a firearm or for any other lawful purpose, is not affected by the absence of an injunction. The possibility of such a public interest therefore does not weigh against the Government's interests in regulating the export of the CAD files.

Although “speech” under the First Amendment is not limited to written or spoken words, *Hurley v. Irish-Am. Gay, Lesbian & Bisexual Grp. of Boston*, 515 U.S. 557, 569 (1995), the Supreme Court has made clear that the First Amendment does not encompass all types of conduct. *See Texas v. Johnson*, 491 U.S. 397, 404 (1989) (“[W]e have rejected ‘the view that an apparently limitless variety of conduct can be labeled ‘speech’ whenever the person engaging in the conduct intends thereby to express an idea’” (quoting *U.S. v. O’Brien*, 391 U.S. 367, 376 (1968))). At a minimum, conduct must be sufficiently expressive and communicative to other persons to qualify for protection under the First Amendment. *See Hurley*, 515 U.S. at 569; *Spence v. Washington*, 418 U.S. 405, 409 (1974))). *Cf. Brown v. Entm’t Merchants Ass’n*, 131 S. Ct. 2729, 2733 (2011) (First Amendment protects video games because they “communicate ideas—and even social messages—through many familiar literary devices (such as characters, dialogue, plot, and music) and through features distinctive to the medium (such as the player’s interaction with the virtual world)”). The ITAR regulations at issue govern the export of defense articles and defense services, including related technical data. As applied to Plaintiffs’ CAD files, the regulations are properly focused on restricting an export that can unquestionably facilitate the creation of defense articles abroad.

The CJ requests submitted by Defense Distributed to DDTC themselves illustrate that the mere publication of ideas is not at issue. According to the CJ requests, the CAD files are functional: “essentially blueprints that can be read by CAD software,” Pl. Br. at App. 208, to “automatically” generate firearms, firearms components, or other defense articles, *id.* at 267.⁹ Further, in its commodity jurisdiction requests, Defense Distributed characterized its role solely in terms of nonexpressive conduct: “Although DD converted this information into CAD file format, DD does not believe that it created any new technical data for the production of the gun.” *Id.* at 211. Plaintiffs’ own description of the items and planned course of conduct thus fails to establish that the export of CAD files is mere “speech” for First Amendment purposes.

The cases on which Plaintiffs rely fail to establish that the law clearly favors their claim

⁹ In the CJ determinations, Defendants concluded that only the CAD files, and not Defense Distributed’s related files (such as “read-me” text files), fell within the commodity jurisdiction of ITAR.

that export of CAD files is an act of protected speech. Plaintiffs rely primarily on *Universal City Studios, Inc. v. Corley*, a Second Circuit copyright decision holding that computer code and computer programs can qualify for First Amendment protection. 273 F.3d 429, 445-49 (2d Cir. 2001). Yet *Corley* expressly distinguished, and thereby recognized the continuing validity of, a prior Second Circuit opinion, *CFTC v. Vartuli*, which held that computer instructions that “induce action without the intercession of the mind or the will of the recipient” are not constitutionally protected speech. 228 F.3d 94, 111 (2d Cir. 2000); see *Corley*, 273 F.3d 448 at n.20 (distinguishing from its holding *Vartuli* and other situations where “a human’s mental faculties do not intercede in executing the instructions”), *id.* at 449 (confirming that code used to communicate to a program user is “not necessarily protected” and that code used to communicate to a computer is “never protected”). Importantly, *Vartuli* held that the fact that some users of the computer instructions at issue might interact with those instructions, rather than simply following them, did not change the constitutional analysis: it was the functionality of the code, not its use, that determined whether the regulations were consistent with the First Amendment.¹⁰ See *Vartuli*, 228 F.3d at 110-12. Plaintiffs’ failure to prove a substantial likelihood of success on this issue alone would be a sufficient basis to deny their motion. See *Suehs*, 692 F.3d at 348.

Further, Plaintiffs’ stated intent to distribute their CAD designs abroad or across U.S. national boundaries also suggests that the First Amendment’s application may be limited here. “It is less [than] clear . . . whether even American citizens are protected specifically by the First Amendment with respect to their activities abroad.” *Laker Airways, Ltd. v. Pan Am. World*

¹⁰ The other two cases cited by Plaintiffs also indicate that code that is purely functional does not warrant First Amendment protection. In *Bernstein v. U.S. Dep’t of Justice*, 176 F.3d 1132, 1139-43 (9th Cir. 1999) and *Junger v. Daley*, 209 F.3d 481, 485 (6th Cir. 2000), the courts held that First Amendment protections extended to computer source code on the theory that it can be read and understood by humans and, unless subsequently compiled, could not directly control the functioning of a computer. See also *Karn v. Dep’t of State*, 925 F.Supp. 1, 9 n.19 (D.D.C. 1996) (computer source code alone is “merely a means of commanding a computer to perform a function”). Even assuming, *arguendo*, that conclusion were correct as to the source code of software here it is undisputed that the CAD files control the functioning of a device. Indeed, here, the CAD files do not merely cause a computer to function generally, but specifically direct a machine to manufacture a firearm and defense articles. Plaintiffs’ reliance on these cases also ignores that the Ninth Circuit opinion in *Bernstein* was subsequently withdrawn and rehearing granted, see *Bernstein v. U.S. Dep’t. of Justice*, 192 F.3d 1308 (9th Cir. 1999), and that, after remand, the plaintiff in *Junger* stipulated to dismissal with prejudice. See Notice of Dismissal, *Junger v. Dep’t of Commerce*, No. 96-cv-1723-JG, Dkt. No. 123 (N.D. Ohio Nov. 16, 2000).

Airways, Inc., 604 F. Supp. 280 (D.D.C. 1984) (finding that aliens have no First Amendment rights abroad); see *Bullfrog Films v. Wick*, 646 F. Supp. 492, 502 (C.D. Cal. 1986) (“No Supreme Court case squarely holds that the First Amendment applies abroad.”); cf. *U.S. v. 12 200-Ft. Reels*, 413 U.S. 123, 125 (1972) (explaining that adjudication of rights at “national borders” implicates “considerations and different rules of constitutional law from domestic regulations”). Even courts that have applied the First Amendment to international speech have recognized that overseas speech or conduct that endangers national security may be outside First Amendment protection. See, e.g., *Haig v. Agee*, 453 U.S. 280, 308 (1981) (even “assuming . . . that First Amendment protections reach beyond our national boundaries,” likelihood of damage to national security rendered speech by a former CIA employee “not protected by the Constitution”); accord *Bullfrog Films*, 646 F. Supp. at 502. Here, where Plaintiffs deliberately seek to use the Internet to distribute CAD files abroad and have made no effort to engage in purely domestic distribution, whether on the Internet or otherwise, their foreign distribution of CAD files may not be protected by the First Amendment.

In any event, the Court need not resolve finally the constitutional question at this stage in light of Plaintiffs’ failure to meet their burden with regard to the other required elements for an injunction. Cf. *Nation Magazine v. Dep’t of Def.*, 762 F. Supp. 1558, 1572 (S.D.N.Y. 1991) (refraining from deciding, absent “a full record,” constitutional questions regarding the First Amendment and military interests abroad). Moreover, as explained below, even assuming that Defense Distributed’s files constitute protected speech, Defendants may properly restrict their export, consistent with the First Amendment.

B. Even If Limiting the Export of CAD Files Implicates the First Amendment, Defendants Are Likely to Prevail on Plaintiffs’ First Amendment Claims.

Plaintiffs’ First Amendment theory relies heavily on the notion that the Internet is merely a means of “publication” of ideas, but this characterization misleads when describing CAD files that generate defense articles and/or their parts with minimum human intervention. Plaintiffs consistently use the terms “publish” or “publication,” see, e.g., Pl. Br. at 1, 5, 8, 13, 14, but in fact it is an “export” that is at issue. ITAR does not prohibit Plaintiffs from distributing these

files to U.S. persons in the United States. Similarly, Defendants have not restricted Plaintiffs' rights to use the Internet to discuss 3D printing, firearms, the Second Amendment, or engage in other expression. Rather, the narrow issue here is Plaintiffs' alleged desire to "facilitat[e] global access" to the CAD files, *i.e.*, to disseminate the automatic ability to make firearms worldwide.

1. ITAR's Export Controls Are a Valid, Content-Neutral Regulation of Plaintiffs' Conduct That Do Not Infringe First Amendment Rights.

Plaintiffs contend that ITAR's export controls on technical data should be subject to strict scrutiny, Pl. Br. at 23-24, but this argument is in error. "[R]egulations that are unrelated to the content of speech" receive less demanding First Amendment scrutiny because they ordinarily "pose a less substantial risk of excising certain ideas or viewpoints from the public dialogue." *Turner Broad. Sys., Inc. v. FCC*, 512 U.S. 622, 642 (1994). And where the Government's purpose in imposing a regulation is "justified without reference to the content of the regulated speech," such regulation is content-neutral. *Clark v. Cmty. for Creative Non-Violence*, 468 U.S. 288, 293 (1984). It is the Government's purpose, not other factors, that is the "controlling consideration" in this determination. *Ward v. Rock Against Racism*, 491 U.S. 781, 791 (1989).

ITAR regulates the conduct of exporting defense articles for the purpose of "further[ing]" world peace [and] the [national] security and foreign policy interests" of the United States, 22 U.S.C. § 2778(a)(1), and Defense Distributed's files function to "automatically" produce such articles or their components. Pl. Br. at App. 267. ITAR's regulation of technical data, particularly Defense Distributed's CAD files, is part and parcel of its regulation of the export of defense articles, a regulation unrelated to the suppression of free expression. *See U.S. v. Chi Mak*, 683 F.3d 1126, 1134-35 (9th Cir. 2012) ("AECA prohibits export without a license of items on the USML without regard to content or viewpoint . . . , defines [] technical data based on its *function*," and is therefore "content-neutral") (emphasis in original); *U.S. v. Edler Indus.*, 579 F.2d 516, 520 (9th Cir. 1978) (recognizing the equivalence for arms control purposes of "military equipment" and the "blueprints specifying the construction of the very same equipment"). The overarching policy objective set forth by Congress and the State Department is to control the spread of defense articles abroad (and related services and technical data)

because munitions and materiel can be used to jeopardize the United States' security interests, a content-neutral interest.¹¹ See *Emergency Coal. to Defend Educ. Travel v. Dep't of Treas.*, 545 F.3d 4, 13-14 (D.C. Cir. 2008).

Plaintiffs' CAD files directly instruct a device to automatically carry out the specified task of manufacturing a defense article. Whatever expressive value may exist in the theory of the CAD files, they indisputably function to create a weapon. Thus, the ITAR may restrict their export on the basis of the *literal* functionality to create the very defense articles that could also indisputably be restricted for export. Moreover, the AECA and ITAR do not attempt in any way to restrict the free flow of public information and ideas about CAD files or 3D printing, either domestically or internationally. See Aguirre Decl. ¶ 30; 22 C.F.R. Part 120. This regulatory scheme is obviously not the product of government hostility toward the spread of ideas about 3D printing of firearms, but rather against the very *means* to easily do so. Accordingly, ITAR's limits on the export of Defense Distributed's CAD files are not directed at the content of expression. See *Chi Mak*, 683 F.3d at 1135; cf. *Capital Cities/ABC, Inc. v. Brady*, 740 F. Supp. 1007, 1013 (S.D.N.Y. 1990) (holding content-neutral a licensing requirement applied to U.S. TV network's broadcasts from Cuba, as part of overall scheme regulating imports and exports).¹² For this reason, strict scrutiny does not apply to a First Amendment analysis of export controls on these CAD files.¹³

¹¹ The government's interest in limiting the distribution of firearms abroad also does not implicate the Second Amendment. Cf. *U.S. v. Huitron-Guizar*, 678 F.3d 1164 (10th Cir. 2012) (rejecting attempt by non-U.S. person to assert Second Amendment rights).

¹² Should the Court conclude, as Defendants contend above, that Plaintiffs' exports are not expressive at all, see *supra* Part II.A, the appropriate standard of review would be rational-basis scrutiny, which ITAR plainly satisfies. See *Voting for Am. v. Steen*, 732 F.3d 382, 392 (5th Cir. 2013) (a statute that "regulate[s] conduct alone and do[es] not implicate the First Amendment" should receive rational-basis scrutiny).

¹³ Also suggesting that the applicable First Amendment protections are reduced is Plaintiffs' characterization of those to whom they wish to supply their CAD files as "customers," Pl. Br. at 27, and Plaintiffs' allegation that their Internet postings of CAD files are intended to "generate revenue." Compl. ¶ 22; see *id.* ¶ 24 (Internet postings would have "generated advertising revenue"). Plaintiffs also discuss "offering . . . items for sale," such as "jigs and code." Pl. Br. at App. 3-4, n.1. Restrictions on "particular type[s] of commercial transaction[s]" are generally treated as regulations of conduct, not speech, see, e.g., *Katt v. Dykhouse*, 983 F.2d 690, 695-96 (6th Cir. 1992); *U.S. v. Bell*, 414 F.3d 474 (3d Cir. 2005). Even if treated as speech, it is well-established that "commercial speech enjoys lesser, intermediate-scrutiny constitutional protection." *RTM Media, L.L.C. v. City of Houston*, 584 F.3d 220, 224 (5th Cir. 2009).

Under intermediate scrutiny, the Government’s regulation of “‘speech’ and ‘non-speech’ elements [] united in a course of conduct” must be sustained if it is “within the constitutional power of the government; it furthers an important or substantial governmental interest; the government interest is unrelated to the suppression of free expression; and the incidental restriction on alleged First Amendment freedoms is no greater than is essential to the furtherance of that interest.” *Kleinman v. City of San Marcos*, 597 F.3d 323, 328 (5th Cir. 2010) (quoting *O’Brien*, 391 U.S. at 376). As the Ninth Circuit held in *Chi Mak*, these standards are met by the “AECA and its implementing regulations,” including ITAR. 683 F.3d at 1135. Regulation of arms trafficking is an “important interest” of the Government with “unquestionable legitimacy.” *Id.* (quoting *Edler*, 579 F.2d at 520). “The technical data regulations substantially advance that interest, unrelated to the suppression of expression, because they set forth clear procedures for seeking approval for export licenses and policies for limiting USML-designation.” *Id.* Nor is the restriction greater than essential: “ITAR makes a point to specifically exclude numerous categories from designation, such as general scientific, mathematical, or engineering papers,” as well as other materials in the public domain. *Chi Mak*, 683 F.3d at 1135; *see U.S. v. Hoffman*, 10 F.3d 808 at *4 (9th Cir. 1993) (unpublished disposition) (if defense articles are “in the public domain, then the AECA does not prohibit their exportation”). Accordingly, even if subjected to a heightened standard of review under the First Amendment, ITAR’s regulation of technical data exports is constitutional. *See id.*; *see also U.S. v. Posey*, 864 F.2d 1487 (9th Cir. 1989).¹⁴

Importantly, the government interests at issue here are the type that merit great deference, even in the context of a First Amendment challenge. *See Kleindienst v. Mandel*, 408 U.S. 753, 766-69 (1972). Courts have recognized that the decision on whether to control a particular commodity for export is one that inherently involves national security and foreign policy judgments that should be left to the discretion of the Executive branch. *See U.S. v. Martinez*, 904

¹⁴ Defendants do not concede that application of strict scrutiny would be fatal to the application of ITAR to Defense Distributed’s CAD files, particularly given that Plaintiffs themselves acknowledge the government interests at issue here as “compelling.” *See* Pl. Br. at 28. In light of the arguments set forth herein, however, Plaintiffs have not met the high burden of persuasion required to obtain a mandatory injunction even under a lesser standard of review. *See Martinez*, 544 F.2d at 1243.

F.2d 601, 602 (11th Cir. 1990); *U.S. v. Mandel*, 914 F.2d 1215, 1223 (9th Cir. 1990). Under Plaintiffs’ broad First Amendment theory, export restrictions on the designs to build a rocket, or software that controls a radar, or technical data concerning missile systems, would all be subject to strict scrutiny on the theory that each such item has informational content as well. *See* Pl. Br. at 23-24. It is no answer to suggest, as Plaintiffs do, that the question turns on whether information is “classified.” *See, e.g.*, Pl. Br. at 11. Courts have squarely rejected this argument:

if the government wished to prevent technical data from being sent to foreign powers, it would be required to suppress the information altogether, at home as well as abroad. This outcome would blur the fact that national security concerns may be more sharply implicated by the export abroad of military data than by the domestic disclosure of such data. Technical data that is relatively harmless . . . when available domestically may, when sent abroad, pose unique threats to national security. It would hardly serve First Amendment values to compel the government to purge the public libraries of every scrap of data whose export abroad it deemed for security reasons necessary to prohibit.

Posey, 864 F.2d at 1496-97. *Cf. Linick v. U.S.*, 104 Fed. Cl. 319, 321 (Fed. Cl. 2012) (Patent Office may “order that an invention be kept secret” if “divulgence might harm national security,” regardless of whether the “Government itself [has] any interest in the invention”).

2. ITAR’s Export Controls Are Not a Facially Unconstitutional Prior Restraint.

Plaintiffs also have no likelihood of success on the merits of their theory that restrictions on the export of the CAD files constitute an unlawful prior restraint on speech. “The doctrine of prior restraint originated in the common law of England, where prior restraints of the press were not permitted, but punishment after publication was.” *Alexander v. U.S.*, 509 U.S. 544, 553 (1993). The classic administrative prior restraint is what is often described as a licensing scheme for speech, where the plaintiff’s right to speak is conditioned on prior approval from the government. *See City of Lakewood v. Plain Dealer Pub. Co.*, 486 U.S. 750, 757 (1988). Such a prior restraint is contrasted with prohibitions on certain speech enforced by punishment *after* the fact, which is not a prior restraint. *See id.* at 764 (distinguishing between statute imposing prohibition on speech and one conditioning speech on obtaining a license or permit). A licensing requirement for conduct that incidentally impacts expression is not such a classic prior restraint, however, and courts have so concluded in the context of the AECA and ITAR, and other prohibitions on imports and exports. *See, e.g., Edler Indus.*, 579 F.2d at 521; *Chi Mak*, 683 F.3d

1136. Cf. *Capital Cities/ABC*, 740 F. Supp. 1007 (upholding against First Amendment challenge licensing requirements applied to international television broadcasts without concluding such a licensing system constituted a prior restraint).¹⁵

Plaintiffs rely heavily on *Freedman v. Maryland*, 380 U.S. 51 (1965)—the case that generally defines the requirements for licensing schemes that affect expression—but both the nature of ITAR and the circumstances here demonstrate that ITAR differs significantly from the prior restraint considered in that case. The “censorship statute” at issue in *Freedman* made it unlawful to exhibit any motion picture unless a state Board of Censors judged the film to be “moral and proper” and not “tend[ing] . . . to debase or corrupt morals or incite to crimes.” 380 U.S. at 52 & n.2. Unlike in *Freedman*, ITAR’s export licensing requirement is not directed at a vast and open-ended category of expressive speech like films, but instead governs the act of providing defense articles or related technical data to those outside the United States (or to foreign persons inside the United States), a much narrower category of conduct that is not characteristically expressive nor remotely comparable to the licensing of adult films domestically. Compare 22 C.F.R. Part 121 (the USML) and 22 C.F.R. § 120.10 (defining technical data) with 380 U.S. at 52; see also *Teague v. Reg’l Comm’r of Customs*, 404 F.2d 441, 446 (2d Cir. 1968) (application of Trading with the Enemy Act, 50 U.S.C. § 5(b) (1964) to academic publications imported from Cuba did not constitute a prior restraint in light of broader regulatory purpose of Act). The Ninth Circuit in *Edler* thus concluded that ITAR’s licensing requirements for technical data, as long as such data is “significantly and directly related to specific articles on the USML,” constitute an appropriate means to “control the conduct of

¹⁵ Plaintiffs’ reliance on opinions of the Department of Justice’s Office of Legal Counsel (“OLC”), Pl. Br. at 3, 18, to support their prior restraint claims is misplaced. These opinions necessarily analyzed the issues at a relatively high level of generality, and do not address the particular application or circumstances presented here. See Pl. Br. at App. 139 (OLC opinions do not “purport to determine the constitutionality of all possible applications of the ITAR”). Thus, Plaintiffs’ lengthy quotation of OLC’s July 1, 1981 opinion regarding “dissemination of technical data,” Pl. Br. at 18, is inapposite. As the July 1, 1981 opinion made clear, its discussion focused on domestic distribution of technical data to foreign persons who might subsequently take that data abroad, for example, “the conversation of a United States engineer who meets with foreign friends at home to discuss matters of theoretical interest,” *id.* at App. 127-28, not a situation like the present where Plaintiffs seek to themselves engage in the overseas transmission of technical data.

assisting foreign enterprises to obtain military equipment and related technical expertise,” and “not an unconstitutional prior restraint on speech.” 579 F.2d at 521.¹⁶

ITAR’s focus on the activity of exporting also mitigates two of the principal concerns raised by classic prior restraint on expression. First, “[b]ecause the censor’s business is to censor,” when the government establishes a censorship board like that in *Freedman* and requires it to determine whether a film is “moral and proper,” it is likely that “the institutional bias of a censorship board . . . [will] lead to the suppression of speech that should be permitted.” *Freedman*, 380 U.S. at 57. In contrast, “laws of general application that are not aimed at conduct commonly associated with expression” do not raise the same concerns about censorship because it will only be a “rare occasion [when] an opportunity for censorship will exist.” *Lakewood*, 486 U.S. at 760-61. Second, laws directing determinations about, e.g., “moral” expression raise concern about whether such discretion is unreviewable. *See City of Littleton v. Z.J. Gifts D-4*, 541 U.S. 774, 782-83 (2004) (upholding licensing scheme that relied on less-subjective criteria than *Freedman*). But where the statute in question regulates general conduct, these concerns are mitigated because “application of the statute to areas unrelated to expression will provide the courts a yardstick with which to measure the licensor’s occasional speech-related decision.” *Lakewood*, 486 U.S. at 761. Indeed, the regulation of the export of technical data in furtherance of national security and foreign policy does not focus on the content of expression, moral or otherwise. And the vast majority of ITAR licensing applications are approved, *see* Aguirre Decl. ¶ 33, demonstrating that there is no “institutional bias of a censor” at issue here. *See id.*¹⁷

¹⁶ Prior restraints are traditionally disfavored in substantial part because it is presumed that after-the-fact punishment is available in the absence of a prior restraint. *See Near v. State of Minn.*, 283 U.S. 697, 718-19 (1931); *Se. Promotions v. Conrad*, 420 U.S. 546, 558-59 (1975). Here, however, such an approach is apt to be inadequate because the ITAR licensing system is intended to prevent irreversible harm to national security and foreign policy that may ensure from export. *See Chi Mak*, 683 F.3d at 1136 (“national security concerns may be more sharply implicated by the export abroad of military data than by domestic disclosure”). In the export context, after-the-fact punishment is likely available only for the exporter because foreign actors making harmful use of military data are likely often to be beyond the reach of U.S. prosecution.

¹⁷ For similar reasons, these statutory criteria are precise enough to avoid the dangers of “a licensing statute placing unbridled discretion” in the hands of DDTC. Pl. Br. at 20-21 (quoting *Lakewood*, 486 U.S. at 757). The unbridled discretion doctrine applies only where a statute or regulation lacks “narrow, objective, and definite standards to guide the licensing authority,” and the Supreme Court has explained that such standards do not require “perfect clarity and precise guidance.” *Forsyth Cnty., Ga. v. Nationalist Movement*, 505 U.S. 123, 131 (1992); *Ward*, 491

3. ITAR's Export Controls Are Not Unconstitutionally Overbroad.

Plaintiffs also raise an “overbreadth” challenge to ITAR’s regulation of technical data. See Pl. Br. at 16-17. Overbreadth is an exception to the prudential standing requirement that a plaintiff may only “assert his own legal rights and interests.” *Warth v. Seldin*, 422 U.S. 490, 499 (1975). In circumstances where a regulation is alleged to be so broad that it is incapable of *any* permissible application, courts may allow a party to bring a facial challenge to a statute because it threatens others not before the court. See *N.Y. State Club Ass’n v. City of New York*, 487 U.S. 1, 14 (1987); *Broadrick v. Oklahoma*, 413 U.S. 601 (1973). Overbreadth is “strong medicine” to be used “sparingly and only as a last resort,” *Broadrick*, 413 U.S. at 613, and a plaintiff must show that the alleged “overbreadth of a statute [is] not only [] real, but substantial . . . judged in relation to the statute’s plainly legitimate sweep.” *Id.* at 615.

Here, Plaintiffs’ overbreadth claim cannot meet these standards. First, “[c]ourts need not entertain an overbreadth challenge ‘where the parties challenging the statute are those who desire to engage in protected speech that the overbroad statute purports to punish.’” *U.S. v. Hicks*, 980 F.2d 963, 969 (5th Cir. 1992) (quoting *Brockett v. Spokane Arcades*, 472 U.S. 491, 504 (1985)). Thus, no overbreadth challenge is “appropriate if the first amendment rights asserted” on behalf of third parties are “essentially coterminous” with those asserted by the plaintiffs themselves. *Id.* Here, as the Supreme Court observed in *Brockett*, “[t]here is . . . no want of a proper party to challenge the [regulations], no concern that the attack on the [regulations] will be unduly delayed or protected speech discouraged.” 472 U.S. at 504. And, indeed, an overbreadth challenge should not properly lie if the regulations have been applied *permissibly* to Plaintiffs, which they have for the reasons outlined above. See *Sec’y State of Md. v. Munson*, 467 U.S. 947, 958 (1984).

Second, even if the merits of Plaintiffs’ overbreadth claim are reached, ITAR’s export

U.S. at 794. As the Ninth Circuit has recognized, the listing of defense articles in the USML and the definition of technical data “delineate narrowly the scope of information subject to arms controls” and thus do not violate the First Amendment. *Chi Mak*, 683 F.3d at 1136; see 22 C.F.R. § 120.10 (defining technical data as the matter “required for the design development, production, manufacture, assembly, operation, repair, testing, maintenance or modification of defense articles . . . includ[ing] . . . blueprints, drawings, photographs, plans, instructions and documentation”); USML Category I(a) (defining included firearms). These criteria provide “adequate standards to guide the official’s decision.” *Thomas v. Chicago Park Dist.*, 534 U.S. 316, 323 (2002).

controls on technical data have a substantially permissible purpose. Plaintiffs have nowhere demonstrated that the regulations have been applied in a substantial number of impermissible ways.¹⁸ To the contrary, the regulations serve the vital purpose of preventing the circumvention of export controls on munitions by the method of providing foreign powers the technical know-how, instructions, blueprints, or—as in the instant case—the automated processes to produce such munitions. *See* Aguirre Decl. ¶ 14. Further, the regulations do not extend to domestic distribution of technical data to U.S. persons and carve out a wide exemption for “public domain” data that helps ensure their reach is appropriately limited. *See* 22 C.F.R. § 120.10(a)(5). For this reason, there is simply no substantial overbreadth here, and Plaintiffs are not likely to succeed on this claim. *See Chi Mak*, 683 F. 3d at 1136 (rejecting overbreadth challenge).

B. Defendants Are Likely to Prevail on Plaintiffs’ Second Amendment Claims.

Plaintiffs are also unable to carry their burden for a mandatory preliminary injunction for their Second Amendment claims because the Court lacks subject matter jurisdiction over these claims, and Plaintiffs have not established that the facts and law are clearly in their favor.

1. Plaintiffs Lack Standing for Their Second Amendment Claims.

According to Plaintiffs, Defendants have infringed upon “two complimentary [sic] guarantees” of the Second Amendment: “the right to acquire arms, and the right to make arms.” Compl. ¶ 49; Pl. Br. at 25-29. Yet none of the Plaintiffs have demonstrated that they have standing to pursue such Second Amendment claims. To establish standing, “a plaintiff must show: (1) it has suffered, or imminently will suffer, a concrete and particularized injury-in-fact; (2) the injury is fairly traceable to the defendant’s conduct; and (3) a favorable judgment is likely to redress the injury.” *Miss. State Democratic Party v. Barbour*, 529 F.3d 538, 544 (5th Cir. 2008) (citation omitted). Plaintiffs must also demonstrate standing for each claim asserted. *DaimlerChrysler v. Cuno*, 547 U.S. 332, 352-53 (2006).

With respect to Defense Distributed, Plaintiffs have failed to establish an injury associated with their claims because they have not set forth any facts indicating that Defense

¹⁸ Indeed, Plaintiffs plead precisely the opposite. *See* Compl. ¶ 24 (“At the time Defense Distributed posted the Published Files, there was no publicly known case of Defendants enforcing a prepublication approval requirement under the ITAR.”).

Distributed's ability to manufacture or acquire arms has been or imminently will be restricted in any way. Rather, Plaintiffs have alleged only a restriction on Defense Distributed's ability to post certain files on its website. *See* Compl. ¶¶ 22-37. Plaintiffs acknowledge that Defense Distributed is in possession of the CAD files that it could use to manufacture firearms or components. *See* Compl. ¶ 37. And Cody Wilson, the "co-founde[r] and now lead[er] [of] Defense Distributed," Pl. Br. at App. 1 ¶ 2, possesses an ATF license to manufacture firearms. *See* BUREAU OF ALCOHOL, TOBACCO, FIREARMS, AND EXPLOSIVES, Listing of Federal Firearms Licensees at lines 61673 & 61675 (May 2015), available at <https://www.atf.gov/file/83411/> (last accessed June 3, 2015).¹⁹ Plaintiffs have therefore failed to set forth specific facts indicating that Defense Distributed's alleged Second Amendment rights have been injured in fact. *See Pub. Citizen, Inc. v. Bomer*, 274 F.3d 212, 218 (5th Cir. 2001).

Plaintiffs have likewise failed to demonstrate that SAF has direct standing to pursue its Second Amendment claims.²⁰ "An organization has standing to sue on its own behalf if it meets the same standing test that applies to individuals." *Henderson v. Stalder*, 287 F.3d 374, 381 (5th Cir. 2002) (citation and internal quotation marks omitted). Plaintiffs do not claim that SAF seeks to manufacture or acquire arms, nor is the suggestion that SAF "would expend its resources to publish and promote" CAD files, Compl. ¶ 38, indicative of a "concrete and demonstrable" injury related to these ostensible Second Amendment rights. *Cf. NAACP v. Kyle, Tex.*, 626 F.3d 233, 238 (5th Cir. 2010). Nor is the alleged injury to SAF fairly traceable to Defendants' conduct, which directly affected Defense Distributed only.

To the extent SAF asserts associational Second Amendment claims, its standing fares no better. *See* Pl. Br. at 28, App. 7; *see also* Compl. ¶ 2. An association lacks standing to bring a claim on behalf of its members unless "its members would otherwise have standing to sue in their own right." *Nat'l Rifle Ass'n v. ATF*, 700 F.3d 185, 191 (5th Cir. 2012) (*NRA*) (citation omitted). SAF cannot meet this test. The members' alleged "keen interest" in the CAD files, *see*

¹⁹ This monthly report is published by ATF as an online spreadsheet. Updates are made available at <https://www.atf.gov/content/firearms/firearms-industry/listing-FFLs>.

²⁰ It is unclear from Plaintiffs' Complaint and motion whether they contend that SAF has direct standing or is asserting associational standing only.

Compl. ¶ 38; *see also* Pl. Br. at App. 6-11, is insufficient to demonstrate that their Second Amendment rights have been injured “in a personal and individual way” as required by Article III. *See Lujan v. Defenders of Wildlife*, 504 U.S. 555, 563 (1992). This is particularly true for the injunctive relief sought here: SAF members’ allegations of future injury, *see* Pl. Br. at App. 9, 11, are purely speculative. *See Lujan*, 504 U.S. at 564; *Osterweil v. Edmonson*, 424 F. App’x 342, 344 (5th Cir. 2011); *Johnson v. Moore*, 958 F.2d 92, 94 (5th Cir. 1992).

Plaintiffs have also failed to establish traceability for any injury to SAF’s members to Defendants’ actions. Accessing and sharing 3D printing files, *see* Pl. Br. at App. 9, 11, is neither a necessary nor sufficient precondition to manufacturing or acquiring arms. Further, Plaintiffs plead that SAF has members “nationwide” only, Compl. ¶ 2, and ITAR does not limit the ability of Defense Distributed or SAF to distribute CAD files directly to U.S. persons within the United States (or otherwise prevent SAF members from acquiring the CAD files). *See Aguirre Decl.* ¶ 16; *cf. Huitron-Guizar*, 678 F.3d at 1169-70. Therefore, any alleged violation of SAF’s members’ Second Amendment rights is not fairly traceable to any action taken by Defendants.²¹

Nor can Plaintiffs obtain standing by “assert[ing] the Second Amendment rights of their customers and website visitors.” Pl. Br. at 27. Plaintiffs have failed to satisfy the requirements for such third-party standing because they have: (1) failed to adequately allege that they themselves suffered an injury in fact; (2) never demonstrated that they have “a close relation” to the unspecified “customers and website visitors”; and (3) not described any hindrance to these customers’ and website visitors’ ability to protect their own interests. *See Bonds v. Tandy*, 457 F.3d 409, 416 n.11 (5th Cir. 2006). In contrast to the cases cited by Plaintiffs, no commercial transaction has occurred and no vendor-vendee relationship appears to exist between Plaintiffs and their “customers.” *Compare* Compl. ¶¶ 5-6 with *Carey v. Population Servs. Int’l*, 431 U.S. 678 (1977) (vendor relationship) and *Reliable Consultants, Inc. v. Earle*, 517 F.3d 738 (5th Cir. 2008) (commercial transactions). More importantly, however, the Fifth Circuit has explained

²¹ Although SAF’s members assert that they have been unable to “locate [firearms files] on Defense Distributed’s website,” they make no allegation that they have attempted to request files from Defense Distributed through other channels, an activity outside the purview of ITAR. *See* Pl. Br. at App. 8-11.

that “*Carey* . . . gives *jus tertii* standing to a party only if the party directly affected is incapable of asserting its own interests.” *Corrosion Proof Fittings v. EPA*, 947 F.2d 1201, 1210 n.6 (5th Cir. 1991), *opinion clarified* (Nov. 15, 1991) (citations omitted). There is no reason to doubt that Plaintiffs’ unspecified “customers and website visitors” are “independent entit[ies], fully capable of asserting their own rights.” *See id.*

2. Plaintiffs Are Unlikely to Succeed on Their Second Amendment Claims.

Assuming Plaintiffs could establish their standing, they have failed to consistently identify the nature of the Second Amendment right that they seek to enforce or a likelihood of success on these claims. Plaintiffs primarily focus on the claim that the Second Amendment encompasses a right to make or acquire arms. Compl. ¶¶ 48-51; Pl. Br. at 26. Elsewhere, they describe the right as “constitutional protection” of “any components necessary to the functioning of one’s constitutionally-protected firearm.” Pl. Br. at 26. At another point, they assert their Second Amendment claim as an infringement on the right to “operate a business that provides Second Amendment services.” Compl. ¶ 49 (quoting *Mance v. Holder*, 2015 WL 567302, at *15 n.8 (N.D. Tex. Feb. 11, 2015); Pl. Br. at 27 (same). Regardless of the Second Amendment right claimed, however, Defendants have at most restricted Defense Distributed’s ability to *export* arms-related technical data, and the Second Amendment does not provide such a right.

The Second Amendment protects “the right of the people to keep and bear Arms.” U.S. Const. amend. II. In *District of Columbia v. Heller*, the Supreme Court held that “the District’s ban on handgun possession in the home violates the Second Amendment, as does its prohibition against rendering any lawful firearm in the home operable for the purpose of immediate self-defense.” 554 U.S. 570, 635-36 (2008). In holding that the Second Amendment secures an individual right, the Court emphasized that the “central right” secured is “to defend oneself in one’s home,” a right that “is not unlimited.” *NRA*, 700 F.3d at 193-94; *Heller*, 554 U.S. at 635.

The Fifth Circuit, like other Courts of Appeals, has adopted a two-step framework for analyzing firearms restrictions challenged on Second Amendment grounds:

[T]he first step is to determine whether the challenged law impinges upon a right protected by the Second Amendment—that is, whether the law regulates conduct that falls within the scope of the Second Amendment’s guarantee; the second step is to

determine whether to apply intermediate or strict scrutiny to the law, and then to determine whether the law survives the proper level of scrutiny.

NRA, 700 F.3d at 194 (citations omitted). “To determine whether a law impinges on the Second Amendment right, we look to whether the law harmonizes with the historical traditions associated with the Second Amendment guarantee.” *Id.* (citing *Heller*, 554 U.S. at 577-628). “If the challenged law burdens conduct that falls outside the Second Amendment’s scope, then the law passes constitutional muster.” *Id.* at 195 (citing *U.S. v. Marzzarella*, 614 F.3d 85, 89 (3d Cir. 2010)). “If the law burdens conduct that falls within the Second Amendment’s scope, we then proceed to apply the appropriate level of means-end scrutiny.” *Id.*

Here, the Court’s inquiry can end at Step One because the challenged regulations do not impose any burden, let alone a substantial burden, on conduct historically protected by the Second Amendment. The Second Amendment’s “central right” is the right to use arms in self-defense in the home, not to export arms across international borders. *Cf. U.S. v. Gurrola-Garcia*, 547 F.2d 1075, 1079 n.6 (9th Cir. 1976) (“Certainly the Second Amendment guarantee of ‘the right of the people to keep and bear Arms’ . . . does not protect the efforts of a person to take munitions across an international border and into a foreign country” (citing *Marchese v. California*, 545 F.2d 645, 647 (9th Cir. 1976))). Restrictions on arms-related exports are “firmly historically rooted,” and therefore harmonize with historic tradition. *See NRA*, 700 F.3d at 204. For example, prior to the Revolution, it was high treason for British subjects to sell arms to the King’s enemies. 4 WILLIAM BLACKSTONE, COMMENTARIES ON THE LAWS OF ENGLAND 82-83 (1769). The early republic similarly placed restrictions on arms-related exports. In 1794, just three years after ratification of the Bill of Rights, “the exportation of munitions of war was prohibited for a year.” 7 JOHN BASSETT MOORE, A DIGEST OF INTERNATIONAL LAW, § 1098 (1906). These restrictions have also been used to advance foreign policy interests during times of peace. In 1902, for example, Congress ratified a treaty with Britain that prevented the export of firearms to certain regions of the Pacific in order to promote international “humanitarian purposes.” 2 MOORE, § 229. These historical restrictions therefore confirm that the “activities covered” by the challenged ITAR provisions are “presumptively not protected from regulation by the Second Amendment.” *NRA*, 700 F.3d at 196 (quoting *Heller v. District of Columbia*, 670

F.3d 1244, 1253 (D.C. Cir. 2011) (*Heller II*)).

Even if the Court concludes that Plaintiffs' claims implicate conduct protected by the Second Amendment, the challenged provisions readily withstand intermediate scrutiny. The Fifth Circuit has applied intermediate scrutiny to laws that, like ITAR's export controls, do not prevent a "law-abiding, responsible adult" from "possess[ing] and us[ing] a handgun to defend his or her home and family," *See id.* at 195 (citations omitted). In applying intermediate scrutiny, the relevant inquiry is "whether there is a reasonable fit between the law and an important government objective." *Id.* at 207. Here, for the same reasons that ITAR's limits on technical data satisfy intermediate scrutiny under the First Amendment, the regulations survive such review under the Second Amendment. *See supra* Part II.B.²² For these reasons, Plaintiffs are unlikely to succeed on their Second Amendment claims.

C. Defendants Are Likely to Prevail on Plaintiffs' Other Claims.

1. ITAR's Standards Are Not Void for Vagueness.

Plaintiffs are also unlikely to succeed in their vagueness challenge to the ITAR's restrictions on the export of defense articles, including "components and parts for firearms" and "technical data" relating to those firearms, components, and parts. These restrictions neither "fail[] to provide [people] of ordinary intelligence fair notice of what is prohibited [n]or . . . authorize[] . . . discriminatory enforcement." *Munn v. Ocean Springs, Miss.*, 763 F.3d 437, 439 (5th Cir. 2014). As explained above, the State Department has enumerated the categories of defense articles for which export is prohibited in the USML, and ITAR specifically defines "technical data" as that which is "required for the design development, production, manufacture, assembly, operation, repair, testing, maintenance or modification of defense articles . . . includ[ing] . . . blueprints, drawings, photographs, plans, instructions and documentation." 22

²² In the nomenclature supplied by *NRA*, ITAR: (1) is "focused on a particular problem," namely, unauthorized exports that pose a danger to national security or foreign policy; (2) implicates a conceded compelling government interest; and (3) employs "means that were reasonably adapted to achieving the objective," by compiling and maintaining on the USML those defense articles and defense services that pose a danger to national security and foreign policy, and reasonably defining "export" to address the ways that items can be disseminated. *See NRA*, 700 F.3d at 208-09; 22 C.F.R. § 120.3, 120.17; *see also* Pl. Br. at 11 ("Nor do Plaintiffs suggest that uploading files to the Internet cannot be viewed, in some sense, as an export."), 28 (acknowledging that interest is compelling).

C.F.R. § 120.10(a). This definition, which accords with the ordinary meaning of the words “technical” and “data,” constitutes a “comprehensible normative standard” in which a “standard of conduct is specified.” *Coates v. City of Cincinnati*, 402 U.S. 611, 614 (1971). If “technical data” as so defined nevertheless “lack[s] the clarity [Plaintiffs] would insist on, it is because . . . ‘we can never expect mathematical certainty from our language.’” *Brown v. Town of Cary*, 706 F.3d 294, 306 (4th Cir. 2013); accord *Munn*, 763 F.3d at 440. In addition, even if an individual were truly uncertain about the definition of “technical data,” that person can apply for a license or submit a CJ request to DDTC. Thus, no one need risk criminal prosecution or civil sanction because it is possible to get an advance determination as to the application of ITAR. See *U.S. Civil Service Comm. v. Nat’l Ass’n of Letter Carriers*, 413 U.S. 548, 580 (1973).

Plaintiffs’ contention that the exclusion of information in the public domain from ITAR renders the regime unconstitutionally vague is even less well-founded. The purpose of the vagueness doctrine in the First Amendment context is to protect against enactments that would limit “the free dissemination of ideas.” *Reeves v. McConn*, 631 F.2d 377, 383 (5th Cir. 1980). Inclusion of the public domain exception in ITAR explicitly promotes the values of free speech and protects First Amendment interests, not the opposite. Similarly, repeal of ITAR’s previous requirement that “[t]he burden for obtaining . . . approval for the publication of technical data . . . is on the [entity] seeking publication,” 49 Fed. Reg. 47,682 (Dec. 6, 1984), see 22 C.F.R. § 125.11 n.3 (1978), lessens any First Amendment harms caused by ITAR, and does not thereby demonstrate that ITAR’s straightforward regulation of exports is impermissibly vague.

2. Application of ITAR’s Export Requirements to Plaintiffs’ CAD Files Does Not Exceed the Statutory Authority Granted by Congress.

Plaintiffs’ claim that Congress has not provided the authority to regulate their transmittal of automated firearms assembly techniques ignores the plain text of the statute. The AECA provides that “the President is authorized to control the import and the export of defense articles and defense services . . . [and] is authorized to designate those items which shall be considered as defense articles and defense services for the purposes of this section and to promulgate regulations for the import and export of such articles and services. The items so designated shall

constitute the USML.” 22 U.S.C. § 2778(a)(1). In doing so, Congress authorized the President to “take into account whether the export of an article would contribute to an arms race, aid in the development of weapons of mass destruction, support international terrorism, increase the possibility of outbreak or escalation of conflict, or prejudice the development of bilateral or multilateral arms control or nonproliferation agreements or other arrangements.” *Id.*

§ 2778(a)(2). In addition, the statute requires that “every person . . . who engages in the business of manufacturing, exporting, or importing any defense articles or defense services designated by the President under subsection (a)(1) of this section shall register with the United States Government agency charged with the administration of this section.” *Id.* § 2778(b)(1)(A)(i). And “[e]xcept as otherwise specifically provided in regulations issued under subsection (a)(1) . . . , no defense articles or defense services designated by the President under subsection (a)(1) . . . may be exported or imported without a license for such export or import.” *Id.* § 2778(b)(2). The plain text of the statute therefore directly authorizes the export licensing scheme at issue here.

Plaintiffs concede that this language provides “authority under the AECA to . . . regulate the export of certain technical data,” and that “uploading files to the Internet can[] be viewed . . . as an export,” but contend that reading these two authorities together—as authorization to regulate technical data on the Internet—is “not what Congress had in mind.” Pl. Br. at 12. But that argument cannot possibly be sustained under a plain reading of the statutory authority. As Defense Distributed itself described in its “Ghost Gunner” application, the technical data in files for that device functions “to automatically find, align, and mill” firearms and their components. *Id.* at App. 267. In the crafting of the AECA, Congress expressed specific concern that “arms transfers [not] become an automatic, unregulated process.” H.R. Rep. No. 94-1144, at 12 (1976), *reprinted in* 1976 U.S.C.C.A.N. 1378, 1388. The regulation of Defense Distributed’s technical data thus fits with Congress’s intent “that the technical data subject to control would be directly relevant to the production of a specified article on the Munitions List.” *Edler Indus.*, 579 F.2d at 521 (noting that the legislative history of AECA’s predecessor statute announced Congress’s direct intention to “allow[] control of munitions, ‘including relevant technical data.’”) (quoting S. Rep. No. 83-1799, at 57 (1954), *reprinted in* U.S.C.C.A.N. 3175, 3244). Thus, Plaintiffs’

ultra vires argument is unpersuasive because it would permit the automatic, “virtual export” of defense articles by anyone willing to undertake the expedient of creating a digital model, sending that digital version abroad, and thereby enabling foreign recipients to “automatically” create an unlimited number of identical copies of the original defense article.²³ Cf. *Edler*, 579 F.2d at 520 (“The authority to regulate arms traffic would be of negligible practical value if it encompassed only the exportation of particular military equipment but not the exportation of blueprints specifying the construction of the very same equipment.”).

Nor do the opinions issued to the State Department by OLC demonstrate that ITAR’s regulations of technical data exceed the scope of authority granted by Congress. To the contrary, the July 1, 1981 OLC opinion recognizes that, under ITAR, the State Department has “traditionally undertaken to regulate the export of technical information” through the technical data provisions. *Id.* Although OLC acknowledged as “somewhat unclear” the delegation of technical data authority, *see* Pl. Br. at App. 125, 129 & nn.7, 11, these opinions are drafted at a high level of generality and nowhere do they state that authority is lacking to regulate matters similar to the CAD files at issue here.²⁴

CONCLUSION

For the foregoing reasons, Plaintiffs’ Motion for a Preliminary Injunction should be denied.

²³ As Plaintiffs note, the State Department’s administration of ITAR and the USML has long subjected technical data, including computer code, to export controls. *See* Pl. Br. at 3; *see also Edler*, 579 F.2d at 519. Congress has repeatedly ratified the USML, incorporating its definitions into subsequent enactments and requiring the Executive to report to Congress in advance of the removal “of any item from the Munitions List.” *See* P.L. 107-228 § 1406; *id.* § 1403; *see also, e.g.*, PL 104-64 § 573 (relying on USML to restrict scope of antiterrorism assistance provided to foreign countries); Omnibus Diplomatic Security and Antiterrorism Act of 1986, P.L. 99-399 § 509(a) (prohibiting export of items on USML to countries providing support for international terrorism). “Congressional actions after the interpretation by the [Executive Branch] . . . indicate acquiescence” where Congress “revisit[s]” a statute without “seek[ing] . . . to change the [] definition.” *Dole v. Petroleum Treathers*, 876 F.2d 518, 522 (5th Cir. 1989); *see also Lorillard v. Pons*, 434 U.S. 575, 580 (1978). Congress has elsewhere ratified ITAR’s definitions of persons subject to its requirements. *See, e.g., U.S. v. Yakou*, 428 F.3d 241, 243-44 (D.C. Cir. 1995).

²⁴ Neither the 1980 official guidance, nor the amendment to ITAR published on December 6, 1984, *see* 49 Fed. Reg. 47,682, indicates that Defendants lack the authority to regulate Plaintiffs’ export of technical data via the Internet. *See* Compl. ¶¶ 19-20. The former makes clear that it is addressing the “publication of data *within the United States*.” The language removed from ITAR by the latter amendment fell within the public domain exemption to ITAR, and concerned only “the publication of technical data” for purposes of placing such data in the public domain. *See* 22 C.F.R. § 125.11(a)(1) n.3 (1978); Pl. Br. App. 200. As explained *supra* Part II.B, publication of technical data is not equivalent to the *export* of such data.

Dated: June 10, 2015

RICHARD L. DURBIN, JR.
Acting United States Attorney
Western District of Texas

ZACHARY C. RICHTER
Assistant United States Attorney
Western District of Texas

Respectfully submitted,

BENJAMIN C. MIZER
Principal Deputy Assistant Attorney General
Civil Division

ANTHONY J. COPPOLINO
Deputy Branch Director
Federal Programs Branch

/s/Eric J. Soskin
ERIC J. SOSKIN
Pennsylvania Bar No. 200663
STUART J. ROBINSON
California Bar No. 267183
Trial Attorneys
United States Department of Justice
Civil Division, Federal Programs Branch
20 Massachusetts Ave., NW
Washington, DC 20530
Phone: (202) 514-9239;
Fax: (202) 616-8460
Email: stuart.j.robinson@usdoj.gov

Attorneys for Defendants

CERTIFICATE OF SERVICE

I certify that on June 10, 2015, I electronically filed this document with the Clerk of Court using the CM/ECF system, which will send notification to

Alan Gura, alan@gurapossessky.com
William B. Mateja, mateja@fr.com
William T. "Tommy" Jacks, jacks@fr.com
David S. Morris, dmorris@fr.com
Matthew Goldstein, matthew@goldsteinpllc.com
Attorneys for Plaintiffs

In addition, I have dispatched this document using the United States Postal Service to the following, who is not listed as a CM/ECF participant:

Josh Blackman
1303 San Jacinto Street
Houston, TX 77002

/s/ Eric J. Soskin

ERIC J. SOSKIN

Trial Attorney

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF TEXAS
AUSTIN DIVISION

DEFENSE DISTRIBUTED, et al.,	§	
Plaintiffs,	§	
	§	
v.	§	No. 1:15-cv-372-RP
	§	
U.S. DEPARTMENT OF STATE, et al.,	§	
Defendants.	§	

Exhibit A: Declaration of Lisa V. Aguirre

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF TEXAS
AUSTIN DIVISION

DEFENSE DISTRIBUTED, et al.,	§	
Plaintiffs,	§	
	§	
v.	§	No. 1:15-cv-372-RP
	§	
U.S. DEPARTMENT OF STATE, et al.,	§	
Defendants.	§	

DECLARATION OF LISA V. AGUIRRE

I, Lisa Aguirre, pursuant to 28 U.S.C. § 1746, hereby declare and say as follows:

1. I am the Director of the Office of Defense Trade Controls Management (DTCM), one of four directors within the Directorate of Defense Trade Controls (DDTC), Bureau of Political-Military Affairs at the Department of State. I have held this position since June, 2013. My roles and responsibilities in this position include managing, overseeing or supporting all DDTC activities.
2. Prior to holding my current position, I was Director of the Office of Defense Trade Controls Compliance in DDTC for over three years, during which time I oversaw numerous DDTC activities, including the management and processing of registration applications and registration fee submissions, reviews of export licenses for prohibited parties, the DDTC Company Visit Program (CVP), a program in which State Department officials visit arms exporters or end users to gather information on compliance with the Arms Export Control Act (AECA) and the International Traffic in Arms Regulations (ITAR), and reviews under the

Committee on Foreign Investment in the United States (CFIUS). As Compliance Director, I also oversaw civil enforcement actions and provided support to criminal enforcement matters under ITAR. In these capacities at DDTC, I have become familiar with the application of the AECA and ITAR as part of DDTC's mission and the full range of DDTC activities in support of its mission.

3. Since joining DDTC, first as a contractor in June 2007, and then through appointment to the federal service in July 2008, I have served continuously in defense trade controls roles.
4. This declaration is submitted in support of the opposition to a motion for preliminary injunction to be filed by the official capacity defendants in the above-captioned case. The information contained herein is based on my personal knowledge and on information provided to me in my official capacity.

Directorate of Defense Trade Controls

5. The Directorate of Defense Trade Controls (DDTC) is part of the Department of State's Bureau of Political-Military Affairs (PM), which reports to the Under Secretary for Arms Control and International Security. DDTC controls the export and temporary import and brokering of defense articles and services covered by the United States Munitions List (USML), in accordance with 22 U.S.C. §§ 2778-2780 of the Arms Export Control Act (AECA) and the International Traffic in Arms Regulations (ITAR) (22 CFR Parts 120-130).

6. DDTC's mission is to carry out the purposes of the AECA to further world peace and the national security and foreign policy of the United States, including by ensuring that commercial defense exports support key objectives of U.S. national security and foreign policy, including weapons nonproliferation, support for allies, and preservation of human rights. DDTC also seeks to ensure that regulation keeps pace with innovation, that U.S. industry and foreign partners comply with applicable policies and requirements, and that the munitions export process is reliable and predictable. DDTC also serves as a resource to the U.S. government, industry, and foreign counterparts on defense trade matters.
7. As part of its mission, DDTC licenses the export and temporary import and brokering of items subject to the International Traffic in Arms Regulations ("ITAR") and seeks to ensure appropriate compliance with, and enforcement of, these regulations. DDTC also maintains, reviews, and clarifies the U.S. Munitions List (USML), and oversees the Commodity Jurisdiction process.
8. The Office of Defense Trade Controls Policy (DTCP) within the Directorate of Defense Trade Controls oversees the development of policy and guidance related to exports of defense articles and services on the USML and subject to the ITAR and the AECA. DTCP manages the interagency Commodity Jurisdiction process, which determines whether or not certain items are controlled on the USML when questions arise concerning whether or not an item is subject to the licensing jurisdiction of the Department of State. DTCP also prepares all changes to the ITAR, which are published in the Federal Register, manages bilateral defense

trade agreements, such as the United Kingdom and Australia Defense Trade Cooperation Treaties, and provides export control policy and regulatory guidance to exporters, defense manufacturers, and foreign allies and partners.

Statutory and Regulatory Framework

9. The Arms Export Control Act (AECA), Section 38(a)(1) (22 U.S.C. 2778(a)(1)), authorizes the President “in furtherance of world peace and the security and foreign policy of the United States . . . to control the import and the export of defense articles and defense services and to provide foreign policy guidance to persons of the United States involved in the export and import of such articles and services. The President is authorized to designate those items which shall be considered as defense articles and defense services for the purposes of this section and to promulgate regulations for the import and export of such articles and services. The items so designated shall constitute the United States Munitions List.”

- (a) The statutory authority of the President to “promulgate regulations for the import and export of such articles and services” has been delegated to the Secretary of State by Executive Order 13637, § 1(n). This delegation requires that “Designations, including changes in designations, by the Secretary of State of items or categories of items that shall be considered as defense articles and defense services subject to export control under section 38 (22 U.S.C. 2778) shall have the concurrence of the Secretary of Defense.”

(b) The authorities under the AECA delegated to the Secretary of State have been further delegated pursuant to Department of State Delegation of Authority 293-2, *Delegation of Authority by the Secretary of State to Officers of the Department of State and the Administrator of the U.S. Agency for International Development of Authorities under the Foreign Assistance Act of 1961 and Other Related Acts* (Oct. 23, 2011), which delegates to the Under Secretary for Arms Control and International Security “the functions conferred on the Secretary by Executive Order 13637 relating to sales and exports under the Arms Export Control Act (22 U.S.C. 2751 *et seq.*).”

10. The ITAR, 22 C.F.R. Chapter I, Subchapter M, Parts 120-130, as amended, 79 Fed. Reg. 77884 (Dec. 29, 2014), implements the AECA. Section 120.1 of the ITAR sets forth how the ITAR is administered:

(a) Section 38 of the Arms Export Control Act (22 U.S.C. 2778), as amended, authorizes the President to control the export and import of defense articles and defense services. The statutory authority of the President to promulgate regulations with respect to exports of defense articles and defense services is delegated to the Secretary of State by Executive Order 13637. This subchapter implements that authority, as well as other relevant authorities in the Arms Export Control Act (22 U.S.C. 2751 *et seq.*). By virtue of delegations of authority by the Secretary of State, these regulations are primarily administered by the Deputy Assistant Secretary of State for Defense Trade Controls, Bureau of Political-Military Affairs.

11. The ITAR provides what particular activities constitute an export. Section 120.17 defines an “export” to mean:

- (1) Sending or taking a defense article out of the United States in any manner, except by mere travel outside of the United States by a person whose personal knowledge includes technical data; or
- (2) Transferring registration, control or ownership to a foreign person of any aircraft, vessel, or satellite covered by the U.S. Munitions List, whether in the United States or abroad; or
- (3) Disclosing (including oral or visual disclosure) or transferring in the United States any defense article to an embassy, any agency or subdivision of a foreign government (*e.g.*, diplomatic missions); or
- (4) Disclosing (including oral or visual disclosure) or transferring technical data to a foreign person, whether in the United States or abroad; or
- (5) Performing a defense service on behalf of, or for the benefit of, a foreign person, whether in the United States or abroad.
- (6) A launch vehicle or payload shall not, by reason of the launching of such vehicle, be considered an export for purposes of this subchapter. However, for certain limited purposes (see § 126.1 of this subchapter), the controls of this subchapter may apply to any sale, transfer or proposal to sell or transfer defense articles or defense services.”¹

¹ On June 3, 2015, the Department of State published in the Federal Register a Notice of Proposed Rulemaking (NPRM) proposing revisions to the ITAR. Among other proposed changes, the Department proposed to clarify the definition of “technical data” by

12. Part 121 of the ITAR sets out those “articles, services, and related technical data” that have been designated as defense articles and defense services pursuant to sections 38 and 47(7) of the AECA. These items make up the USML. There are 21 categories on the USML under which a particular item may be designated as a defense article.
13. As relevant to this litigation, under Category I, *Firearms, Close Assault Weapons and Combat Shotguns*, the following items are designated as defense articles:
 - (a) Non-automatic and semi-automatic firearms to caliber .50 inclusive (12.7 mm).
 - (b) Fully automatic firearms to .50 caliber inclusive (12.7 mm).
 - (c) Firearms or other weapons (e.g., insurgency-counterinsurgency, close assault weapons systems) having a special military application regardless of caliber.
 - (d) Combat shotguns. This includes any shotgun with a barrel length less than 18 inches.
 - (e) Silencers, mufflers, sound and flash suppressors for the articles in (a) through (d) of this category and their specifically designed, modified or adapted components and parts.
 - (f) Riflescopes manufactured to military specifications. (See category XII(c) for controls on night sighting devices.)
 - (g) Barrels, cylinders, receivers (frames) or complete breech mechanisms for the articles in paragraphs (a) through (d) of this category.
 - (h) Components, parts, accessories and attachments for the articles in paragraphs (a) through (g) of this category.

specifying that technical data may take the form of, inter alia, CAD files. In addition, to make more explicit the existing control on exports, the Department proposed to add a paragraph specifying that providing technical data on a publicly-accessible network, such as the Internet, is an export because of its inherent accessibility to foreign powers. The Department has requested that interested parties submit comments on these and other elements of the proposed rulemaking between June 3 and August 3, 2015. See Exhibit 7.

- (i) Technical data (as defined in § 120.10 of this subchapter) and defense services (as defined in § 120.9 of this subchapter) directly related to the defense articles described in paragraphs (a) through (h) of this category. Technical data directly related to the manufacture or production of any defense articles described elsewhere in this category that are designated as Significant Military Equipment (SME) shall itself be designated SME.
 - (j) The following interpretations explain and amplify the terms used in this category and throughout this subchapter:
 - (1) A firearm is a weapon not over .50 caliber (12.7 mm) which is designed to expel a projectile by the action of an explosive or which may be readily converted to do so.
 - (2) A rifle is a shoulder firearm which can discharge a bullet through a rifled barrel 16 inches or longer.
 - (3) A carbine is a lightweight shoulder firearm with a barrel under 16 inches in length.
 - (4) A pistol is a hand-operated firearm having a chamber integral with or permanently aligned with the bore.
 - (5) A revolver is a hand-operated firearm with a revolving cylinder containing chambers for individual cartridges.
 - (6) A submachine gun, "machine pistol" or "machine gun" is a firearm originally designed to fire, or capable of being fired, fully automatically by a single pull of the trigger.
14. In addition to the inclusion of "technical data" for Category I defense articles on the USML, there are several other provisions of the ITAR related to "technical data."
- a. Section 120.10 of the ITAR defines "technical data" as "(a)(1) Information, other than software as defined in § 120.10(a)(4) which is required for the design, development, production, manufacture,

assembly, operation, repair, testing, maintenance or modification of defense articles. This includes information in the form of blueprints, drawings, photographs, plans, instructions or documentation[;] (2) Classified information relating to defense articles and defense services on the U.S. Munitions List and 600-series items controlled by the Commerce Control List; (3) Information covered by an invention secrecy order; or (4) Software (see § 120.45(f)) directly related to defense articles.² (b)³ The definition in paragraph (a) of this section does not include information concerning general scientific, mathematical, or engineering principles commonly taught in schools, colleges, and universities, or information in the public domain as defined in § 120.11 of this subchapter or telemetry data as defined in note 3 to Category XV(f) of part 121 of this subchapter. It also does not include basic marketing information on function or purpose or general system descriptions of defense articles.”

- b. Section 120.6 of the ITAR defines a “defense article” as “any item or technical data designated in § 121.1 of this subchapter. This term includes technical data recorded or stored in any physical form, models, mockups or other items that reveal technical data directly relating to items designated in § 121.1 of this subchapter. It also includes forgings, castings, and other unfinished products, such as

² This sentence added by 79 FR 61226 (Oct. 10, 2014).

³ Amended by 79 FR 27180 (May 13, 2014, effective Nov. 10, 2014), as corrected by 79 FR 66608 (Nov. 10, 2014).

extrusions and machined bodies, that have reached a stage in manufacturing where they are clearly identifiable by mechanical properties, material composition, geometry, or function as defense articles.⁴ It does not include basic marketing information on function or purpose or general system descriptions.”

- c. Section 120.9 of the ITAR defines a “defense service” as “(1) The furnishing of assistance (including training) to foreign persons, whether in the United States or abroad in the design, development, engineering, manufacture, production, assembly, testing, repair, maintenance, modification, operation, demilitarization, destruction, processing or use of defense articles; (2) The furnishing to foreign persons of any technical data controlled under this subchapter (see § 120.10), whether in the United States or abroad; or (3) Military training of foreign units and forces, regular and irregular, including formal or informal instruction of foreign persons in the United States or abroad or by correspondence courses, technical, educational, or information publications and media of all kinds, training aid, orientation, training exercise, and military advice. (See also § 124.1.)”
- d. Collectively, the “technical data” provisions serve the purpose of limiting the export of detailed information needed to manufacture, maintain, or operate defense articles controlled on the USML. Such

⁴ This sentence was added to the definition of defense article by 79 FR 61226 (Oct. 10, 2014).

export limitations advance the purposes of the AECA by limiting the ability of foreign powers to design, develop, and produce defense articles in lieu of being able to obtain those articles directly. Absent the inclusion of technical data in the ITAR, the ITAR's limits on arms transfers would be of negligible practical effect because the ITAR would leave unregulated the exportation of the fundamental technology, know-how, blueprints, and other design information sufficient for foreign powers to construct, produce, manufacture, maintain, and operate the very same equipment regulated in its physical form by the ITAR.

15. The ITAR also sets forth the policy on designating and determining how a specific article or service may be designated as a defense article or defense service.

- a. Pursuant to section 120.3, a particular article or service will be designated as a defense article if it: “(1) Meets the criteria of a defense article or defense service on the U.S. Munitions List; or (2) Provides the equivalent performance capabilities of a defense article on the U.S. Munitions List.”
- b. Section 120.3 also provides that a specific article or service “shall be determined in the future as a defense article or defense service if it provides a critical military or intelligence advantage such that it warrants control” under the ITAR.

c. Section 120.3 also specifies that the “intended use of the article or service after its export (*i.e.*, for a military or civilian purpose), by itself, is not a factor in determining whether the article or service is subject to the controls of this subchapter.”

16. ITAR jurisdiction extends only to the export of defense articles, defense services, and technical data. For this reason, ITAR does not limit the ability of Defense Distributed or others to distribute CAD files to U.S. persons within the United States for domestic use.

The Commodity Jurisdiction (CJ) process

17. Commodity Jurisdictions, commonly referred to as “CJs,” are the determination made by the Department of State identifying the export control jurisdiction of goods, services and information.
18. The purpose of these determinations is to reach a conclusion as to whether, for purposes of export controls, goods, services, or information are under the jurisdiction of the Department of State pursuant to ITAR or under the jurisdiction of the Department of Commerce, which administers the Export Administration Regulations (EAR).⁵

⁵ A few categories of goods, services, or information are under the jurisdiction of the Department of Energy, Department of Homeland Security, or another Executive Branch agency. Goods, services, or information may also be within the public domain and not subject to export controls at all.

19. Section 120.4 of the ITAR establishes the CJ procedure,⁶ which “is used with the U.S. Government if doubt exists as to whether an article or service is covered by the U.S. Munitions List. It may also be used for consideration of a re-designation of an article or service currently covered by the U.S. Munitions List. The Department must provide notice to Congress at least 30 days before any item is removed from the U.S. Munitions List.” As required by Section 120.4, the determination “entails consultation among the Departments of State, Defense, Commerce, and other U.S. Government agencies and industry in appropriate cases.” In the vast majority of circumstances, the CJ procedure is unnecessary because there is no doubt as to whether an item to be exported is a defense article or defense service.

20. Section 120.4 of the ITAR sets forth the criteria for making a CJ determination: A designation that an article or service meets the criteria of a defense article or defense service, or provides the equivalent performance capabilities of a defense article on the U.S. Munitions List set forth in this subchapter, is made on a case-by-case basis by the Department of State, taking into account:

(i) The form and fit of the article;⁷ and

⁶ See 58 FR 39283, July 22, 1993, as amended at 71 FR 20536, Apr. 21, 2006; 75 FR 46843, Aug. 4, 2010; 78 FR 22753, Apr. 16, 2013; 79 FR 8084, Feb. 11, 2014.

⁷ The form of a commodity is defined by its configuration (including the geometrically measured configuration), material, and material properties that uniquely characterize it. The fit of a commodity is defined by its ability to physically interface or connect with or

(ii) The function and performance capability of the article.⁸

21. Section 120.4(f) further requires that “State, Defense and Commerce will resolve commodity jurisdiction disputes in accordance with established procedures. State shall notify Defense and Commerce of the initiation and conclusion of each case.”
22. Section 120.4(g) provides an avenue for appeal of a CJ determination:

A person may appeal a commodity jurisdiction determination by submitting a written request for reconsideration to the Deputy Assistant Secretary of State for Defense Trade Controls. The Deputy Assistant Secretary's determination of the appeal will be provided, in writing, within 30 days of receipt of the appeal. If desired, an appeal of the Deputy Assistant Secretary's decision can then be made to the Assistant Secretary for Political-Military Affairs.
23. DTCP considers a variety of information in its consideration of CJ requests, including the information attached to the request (such as product brochures, technical specifications and/or blue prints, sales information, etc.), the USML category in which an item most likely may fit, previous CJs on the technology or related matters, and previously-issued export licenses for similar items.

become an integral part of another commodity. [See Note 1 to paragraph (d), section 120.4 of the ITAR.

⁸ The function of a commodity is the action or actions it is designed to perform. Performance capability is the measure of a commodity's effectiveness to perform a designated function in a given environment (e.g., measured in terms of speed, durability, reliability, pressure, accuracy, efficiency).

After DTCP prepares a preliminary analysis, the CJ request and preliminary analysis are circulated to the relevant interagency partners for consultation.

Defense Distributed's CJ Requests

24. In early May, 2013, DTCP became aware through media reports that Defense Distributed (DD), a pending 501(c)(3) non-profit corporation located in Austin, Texas, had placed on an unrestricted website executable Computer Aided Design (CAD) files enabling the manufacture of plastic firearm components, accessories, and attachments with a 3D printer. *See, e.g.*, Exhibit 1.
25. As a result, the Department of State's Office of Defense Trade Controls Compliance (DTCC) became concerned that these files might be subject to the ITAR, in which case DD might be exporting these files without authorization. DTCC therefore sent a letter to DD, suggesting that they remove the files from their website and submit CJ requests to determine whether the files were controlled by the ITAR. *See* Exhibit 2. DD complied with the request and on June 21, 2013, submitted ten CJ requests. *See* Exhibit 3.
26. In its CJ submission, DD identified a number of publicly available sources for information on how to manufacture firearms and related components, including books on gunsmithing and gun design blueprints and schematics available in a variety of media, including on the Internet. DD asserted that their CAD files were no different from any other medium that contains basic manufacturing "know

how” for firearms, and that these files should be found to be in the public domain and not controlled under the ITAR. *See* Exhibit 3.

27. In addition to conferring with other agencies in accordance with ITAR Section 120.4, DTCP sought to better understand additive manufacturing and 3D printing hardware and technology and its evolution and diffusion, the impact of the availability of CAD files (and other, similar data files) on the enforcement of export controls, and the application of multilateral export control regime, particularly the Wassenaar Arrangement on Export Controls on Conventional Arms and Dual-use Goods and Technologies, to such files and technologies. DTCP consulted other State Department offices and U.S. government agencies to benefit from their expertise and consideration of these technologies and issues. In addition, DTCP organized a conference on additive manufacturing/3D printing technology in March 2014.

28. In January 2015, while consideration of DD’s June, 2013 CJ requests was ongoing, DD submitted a CJ request for the “Ghost Gunner,” a computer numerically controlled (CNC) press for milling metal firearms components. *See* Exhibit 4. On April 15, 2015, DDTC responded by providing a CJ determination to Defense Distributed, finding that the Ghost Gunner would not be subject to the jurisdiction of the Department of State. *See* Exhibit 5. In the course of consideration of the Ghost Gunner, DTCP determined that project files and data files for producing a defense article on a 3D printer or similar device constituted technical data on that defense article that would be subject to ITAR jurisdiction.

Resolution of the Ghost Gunner CJ request also helped DTCP conclude the CJ process for DD's June 21, 2013 CJ requests. On June 4, 2015, DTCP provided CJ determinations for the requested items. See Exhibit 6.

DDTC's CJ Determination

29. In making its CJ determination, DDTC identified several factors that warrant treatment of DD's CAD files as technical data subject to ITAR jurisdiction.
- a. The central function of DD's executable CAD files appears to be to enable the manufacture of end-items that are ITAR-controlled defense articles.
 - b. As DD described in its Ghost Gunner CJ request, DD's CAD files can be used to "automatically find, align, and mill" a defense article such as a firearm on a 3D printer or other manufacturing device. Manufacture of a defense article in this way requires considerably less know-how than manufacture in reliance on conventional technical data, which merely *guides* the manufacture of a defense article and requires additional craftsmanship, know-how, tools, and materials.
 - c. Although DD contended that the technical data constituted published data already in the public domain, the existing material in the public domain identified by DD did not include CAD files that could be used to automatically generate defense articles. Because CAD files provide the

additional functionality described above, DD's CAD files are a meaningful step beyond previous, public-domain material.

- d. In addition, because DD's CAD files are information similar to "blueprints, drawings, photographs, plans, instructions or documentation" that can be used to automatically manufacture defense articles, DDTC concluded that the regulations place them within ITAR commodities jurisdiction.

30. Based on these considerations, its consultations with other State Department offices and U.S. government agencies, its own expertise, and the text of the AECA and ITAR, DDTC concluded that DD's CAD files fall within the jurisdiction of the ITAR as technical data under Category I, subsection (i) of the USML, relying on the definition of technical data in 22 C.F.R. § 120.10(a)(1). DDTC concluded that other information, including a "read-me" file submitted by DD for a CJ determination, did not fall within the jurisdiction of the ITAR. Accordingly, DDTC's determination does not restrict DD from discussing information and ideas about 3D printing, either domestically or internationally, as long as such discussions do not include the export of technical data.

31. Classification of DD's CAD files as within the jurisdiction of the ITAR is not an outright prohibition on the export of these files. Rather, ITAR requires that DD obtain a "license or other approval . . . pursuant to the ITAR prior to any export" for these CAD files.

32. Should DD submit an application for approval to export its CAD files, DDTC will review the proposed export, including its intended recipients and the type, form, and scope of the export. DDTC will consider the application in accordance with the factors enumerated in 22 C.F.R. § 126.7, including whether such export is prohibited “by any statute of the United States.” 22 C.F.R. § 126.7(a), whether such export would be “in furtherance of world peace, the national security or the foreign policy of the United States.” 22 C.F.R. § 126.7(a)(1), whether “[a]n applicant, any party to the export or agreement, any source or manufacturer of the defense article or defense service or any person who has a significant interest in the transaction has been debarred, suspended, or otherwise is ineligible to receive an export license or other authorization from any agency of the U.S. government.” *id.* § 126.7(a)(6). In addition, there are numerous countries to which exports of some or all categories of defense articles are prohibited. *See, e.g.*, 22 C.F.R. § 126.1.

33. In my experience, the overwhelming majority of ITAR licensing applications are approved outright or approved with conditions intended to safeguard the defense article being exported from use in a way that would damage world peace or the national security or foreign policy interests of the United States. Of course, any given licensing application will only be approved if the application satisfies the standards required under 22 C.F.R. § 126.7.

Likely Effects of the Preliminary Injunction Sought by Plaintiffs

34. The entry of a preliminary injunction authorizing the posting of DD's CAD files to the Internet without restriction would make those files available worldwide to any Internet user, thereby permitting the export of those files to any foreign person or foreign power with access to DD's website. Such an injunction would deny DDTC the opportunity to consider, among other things, whether any specific export of DD's CAD files would violate the law or would cause significant harm to the national security or foreign policy interests of the United States.

35. Absent a specific request for an export license, I have considered the likely impacts of an unrestricted export of DD's CAD files to any interested person, entity, or foreign power and concluded that the likely effect of a preliminary injunction would be to cause significant harm to the national security and foreign policy interests of the United States. Although a comprehensive enumeration of the possible harms would be difficult, I can identify the following as among the most concerning:

- a. The "Liberator" firearm included in DD's CAD designs presents a specific and unique risk to the national security and foreign policy interests of the United States. The Liberator is a plastic firearm which can be produced in a way as to be both fully operable and virtually undetectable by conventional security measures such as metal detectors. police and security services, could particularly, (though not uniquely) cause damage U.S. foreign policy interests. If U.S.-origin CAD files were used to

manufacture an undetectable “Liberator” in a foreign country, and that weapons was then used to commit an act of terrorism, piracy, assassination, or other serious crime (e.g., to compromise aviation security overseas), the act itself – or the interests of a foreign country in holding the United States accountable – could cause serious and long-lasting harm to the foreign policy and national security interests of the United States.⁹

- b. The United States and other countries rely on international arms embargoes, export controls, and other measures to restrict the availability of defense articles sought by terrorist organizations. Making DD’s CAD files available through unrestricted access on the Internet would provide any such organization with defense articles, including firearms, at its convenience, subject only to its access to a 3D printer, an item that is widely commercially available. Terrorist groups and other actors could then potentially manufacture and use such weapons against the United States or its allies.
- c. Making DD’s CAD files available through unrestricted access on the Internet would likewise provide access to the firearms components and replacement parts to armed insurgent groups, transnational organized criminal organizations, and states subject to U.S. or UN arms embargoes.

⁹ Undetectable firearms are unlawful in the United States pursuant to the Undetectable Firearms Act of 1988. See 18 U.S.C. § 922(p). Although the “Liberator” design includes insertion of a six-ounce piece of metal to make it detectable by metal detectors, this metal content can be removed without rendering it inoperable, thereby permitting it to be both operable and undetectable.

Access to weapons technology coupled with the uncontrolled and increasingly ubiquitous means of production (i.e., 3D printers or other similar manufacturing technology capable of executing CAD files) could contribute to armed conflict, terrorist or criminal acts, and seriously undermine global export control and non-proliferation regimes designed to prevent the dangerous and destabilizing spread and accumulation of weapons and related technologies. U.S. leadership in these areas also would suffer, contributing overall to a more dangerous international environment.

- d. Many countries, including important U.S. allies, have more restrictive firearms laws than the United States and have identified firearms CAD files for 3D printers as a threat to domestic firearms laws. For example, both the United Kingdom and Japan have arrested individuals for manufacturing or attempting to use firearms CAD files and 3D printers to manufacture firearms. *See, e.g.,* <http://www.bbc.com/news/technology-27322947>, accessed, June 6, 2015. Unrestricted exports from the United States of munitions or technical data, such as DD's CAD files, which could be used to automatically manufacture a firearm or other defense article, would undercut the domestic laws of these nations, increase the risk of domestic violence in those countries, and thereby damage U.S. foreign relations with those countries and foreign policy interests.

36. In my judgment, the entry of a preliminary injunction in this matter would increase the risk of all of the foregoing harms. Indeed, such an injunction could reasonably be expected to bring attention to DD's CAD files, making awareness of their capabilities and accessibility known more widely to individuals, entities, and foreign powers that would make use of DD's CAD files to the detriment of U.S. foreign policy and national security interests.

I declare under penalty of perjury that the foregoing is true and correct.

Executed on June 10, 2015.

A handwritten signature in cursive script, reading "Lisa V. Aguirre", is written above a horizontal line.

Lisa V. Aguirre

EXHIBIT

1

3D-printable guns are just the start, says Cody Wilson

The inventor of 'The Liberator' plastic firearm believes in an open future and the 'complete explosion' of all gun law

Alex Rayner

Monday 6 May 2013 11.56 EDT

Cody Wilson is a polite, 25-year-old law student at the University of Texas in Austin, with dark, close-cropped hair and a forward, affable charm. This week he plans to release the blueprint for a gun that can be downloaded from the internet and produced using a 3D printer.

He and his friends have spent almost a year developing the Liberator, a "Wiki weapon" that can be assembled from components made on an \$8,000 (£5,150) printer that they bought on eBay. Using files shared online, the machine creates the solid parts from layers of plastic.

Wilson's group, Defense Distributed, thinks everyone should have access to a gun and is working to make it possible through Defcad.org, a depository for weapons designs. It was set up in December after its files were removed from another site following the Sandy Hook elementary school shootings. In March, Wilson was issued a federal firearms licence, allowing him to make guns legally.

"I come from a typical middle class family, for the United States in the south: religious parents, conservative values, though we didn't own a lot of firearms," he says. "We had one shotgun that we never really used."

Despite buying a shotgun shortly after turning 21, Wilson says it was his studies, first as an English literature major, then as a law student, that started his interest in the politics of weapons ownership. "I read [19th-century French anarchist theorist Pierre-Joseph] Proudhon," he says, "I like Jean Baudrillard. I like their critiques of mass culture."

He admits that, given current technology, printing a gun is the least effective way of obtaining a firearm, and that it is easier to simply fashion a gun from the contents of any hardware store.

Yet he half hopes, half believes that soon, thanks to the convergence of file-sharing and 3D printing, there will come about "a complete explosion of all available gun laws. I think we should be allowed to own automatic weapons; we should have the right to own all the

terrible implements of war, as [American political philosopher] Fench Coxé said, and I think this principle probably applies globally."

A self-described child of the internet age, Wilson is an admirer of Julian Assange and Kim Dotcom. "I number myself among them, at least in spirit," he says. "I think the future is openness to the point of the eradication of government. The state shouldn't have a monopoly on violence; governments should live in fear of their citizenry."

His ambitions don't stop at firearms. Ultimately, he wants to turn Defcad into "the world's first unblockable open-source search engine for all 3D printable parts", a Pirate Bay-style archive not only for printable pistols, but for everything from prosthetic limbs to drugs and birth-control devices.

More features

Topics

US gun control

Shots fired from world's first 3D-printed handgun

Cody Wilson, 25, successfully tested plastic handgun built by his Texas firm Defense Distributed using an \$8,000 3D printer

Adam Gabbatt in New York

Monday 6 May 2013 14.43 EDT

The world's first gun made almost entirely by a 3D plastic printer has been successfully fired in Texas.

The successful test of the plastic handgun, which was built by Defense Distributed using an \$8,000 3D printer, came after a year of development. The company, which is run by 25-year-old Cody Wilson, now plans to publish the blueprints for the gun online.

Wilson and a companion successfully fired the gun for the first time in Austin, Texas, at the weekend, Forbes reported. A video published online shows the gun held in place by a metal stand, with yellow string attached to its trigger. By yanking on the string, the pair were able to pull the trigger from 20ft away, successfully discharging a .380 caliber bullet.

Defense Distributed's device is controversial because of the way it is made. Fifteen of its 16 pieces were constructed in a second-hand Stratasys Dimension SST 3D printer, Forbes said. The final piece, the firing pin, is a common nail available from any hardware store. The printer used ABS plastic to create the gun parts, which were then slotted together by Wilson. After Forbes's revelation, the BBC filmed a later test, in which Wilson successfully fired the gun by hand.

The Undetectable Firearms Act of 1988 makes it illegal to manufacture in the US any firearm that is not detectable by walk-through metal detectors. To combat this, Wilson inserted a 6oz piece of steel into the body of his gun, making it legal.

How long the law stays this way remains to be seen, however. On Sunday, New York senator Charles Schumer called for legislation to make building a gun with a 3D printer illegal, and said he and the New York congressman Steve Israel would introduce the Undetectable Firearms Modernisation Act, which would ban weapons like Wilson's.

Such an act would not be the first setback for Wilson, a law student at the University of Texas. An attempt to raise money for the 3D printed gun project through Indiegogo was thwarted when the crowdfunding website took his pitch offline, citing a breach of rules. After Wilson raised \$20,000 through Bitcoin donations, he was hindered again when

Stratys seized back his printer.

Defense Distributed acquired a second-hand Stratys, however, and carried on experimenting. Wilson successfully made and tested parts of an AR-15 semi-automatic rifle - the weapon which has been used in a number of mass shootings in the US - before turning his attention to a plastic handgun.

More news

Topics

US gun control

3D printing

3D

EXHIBIT

2



United States Department of State
Bureau of Political-Military Affairs
Office of Defense Trade Controls Compliance
Washington, D.C. 20522-0112

MAY 08 2013

In reply refer to
DTCC Case: 13-0001444

Mr. Cody Wilson
Defense Distributed
711 W. 32nd Street, Apt. 115
Austin, TX 78705

Dear Mr. Wilson:

The Department of State, Bureau of Political Military Affairs, Office of Defense Trade Controls Compliance, Enforcement Division (DTCC/END) is responsible for compliance with and civil enforcement of the Arms Export Control Act (22 U.S.C. 2778) (AECA) and the AECA's implementing regulations, the International Traffic in Arms Regulations (22 C.F.R. Parts 120-130) (ITAR). The AECA and the ITAR impose certain requirements and restrictions on the transfer of, and access to, controlled defense articles and related technical data designated by the United States Munitions List (USML) (22 C.F.R. Part 121).

DTCC END is conducting a review of technical data made publicly available by Defense Distributed through its 3D printing website, DEFCAD.org, the majority of which appear to be related to items in Category I of the USML. Defense Distributed may have released ITAR-controlled technical data without the required prior authorization from the Directorate of Defense Trade Controls (DDTC), a violation of the ITAR.

Technical data regulated under the ITAR refers to information required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance or modification of defense articles, including information in the form of blueprints, drawings, photographs, plans, instructions or documentation. For a complete definition of technical data, see § 120.10 of the ITAR. Pursuant to § 127.1 of the ITAR,

it is unlawful to export any defense article or technical data for which a license or written approval is required without first obtaining the required authorization from the DDTC. Please note that disclosing (including oral or visual disclosure) or transferring technical data to a foreign person, whether in the United States or abroad, is considered an export under § 120.17 of the ITAR.

The Department believes Defense Distributed may not have established the proper jurisdiction of the subject technical data. To resolve this matter officially, we request that Defense Distributed submit Commodity Jurisdiction (CJ) determination requests for the following selection of data files available on DEFCAD.org, and any other technical data for which Defense Distributed is unable to determine proper jurisdiction:

1. Defense Distributed Liberator pistol
2. .22 electric
3. 125mm BK-14M high-explosive anti-tank warhead
4. 5.56/.223 muzzle brake
5. Springfield XD-40 tactical slide assembly
6. Sound Moderator – slip on
7. “The Dirty Diane” 1/2-28 to 3/4-16 STP S3600 oil filter silencer adapter
8. 12 gauge to .22 CB sub-caliber insert
9. Voltlock electronic black powder system
10. VZ-58 front sight.

DTCC/END requests that Defense Distributed submit its CJ requests within three weeks of receipt of this letter and notify this office of the final CJ determinations. All CJ requests must be submitted electronically through an online application using the DS-4076 Commodity Jurisdiction Request Form. The form, guidance for submitting CJ requests, and other relevant information such as a copy of the ITAR can be found on DDTC’s website at <http://www.pmddtc.state.gov>.

Until the Department provides Defense Distributed with final CJ determinations, Defense Distributed should treat the above technical data as ITAR-controlled. This means that all such data should be removed from public access immediately. Defense Distributed should also review the remainder of the data made public on its website to

- 3 -

determine whether any additional data may be similarly controlled and proceed according to ITAR requirements.

Additionally, DTCC/END requests information about the procedures Defense Distributed follows to determine the classification of its technical data, to include the aforementioned technical data files. We ask that you provide your procedures for determining proper jurisdiction of technical data within 30 days of the date of this letter to Ms. Bridget Van Buren, Compliance Specialist, Enforcement Division, at the address below:

Office of Defense Trade Controls Compliance
PM/DTCC, SA-1, Room L132
2401 E Street, NW
Washington, DC 20522
Phone: 202-663-3323.

We appreciate your full cooperation in this matter. Please note our reference number in any future correspondence.

Sincerely,



Glenn E. Smith
Chief, Enforcement Division

EXHIBIT

3

WILLIAMS MULLEN

Jahna M. Hartwig
Direct Dial: 202.293-8145
jhartwig@williamsmullen.com

June 21, 2013

Ms. Sarah Heidema
U.S. Department of State
Directorate of Defense Trade Controls
PM/DDTC, SA-1, Room 1200
2401 E Street, NW
Washington, DC 20037

Subject: Commodity Jurisdiction Requests for Data Files Posted by Defense Distributed

Enclosures: (1) Printouts of Drawings from Files Posted at DEFCAD.org
(2) Wikipedia Page for 125mm BK-14M HEAT
(3) Thingiverse Page for Sound Moderator
(4) Thingiverse Page for VZ-58 Front Sight
(5) Examples of Solvent Trap Adapters
(6) Examples of CAD Files for .22 Pistols
(7) Examples of CAD Files for Muzzle Brakes
(8) Examples of CAD Files for Slide Assemblies
(9) Examples of CAD Files for Voltlock System

Dear Ms. Heidema:

Defense Distributed has been requested by DTCC/END to submit requests for commodity jurisdiction determinations in connection with Case No. 13-0001444 for ten sets of data files posted to DEFCAD.org. As demonstrated below, the files are primarily Computer Aided Design (CAD) data files and should be considered public domain information that is excluded from the ITAR pursuant to Section 120.11. Defense Distributed therefore respectfully requests a determination that these files are not subject to the ITAR.

COMMODITY DESCRIPTIONS

Each of these Commodity Jurisdiction requests relates to data files, almost all of which are essentially blueprints that can be read by CAD software. A description of each file or set of files is set out below. The files are in one of the following formats:

- STL (STereoLithography or Standard Tessellation Language) is a file format native to the stereolithography CAD software and can be used with some 3D printers. "Stereolithography" is a means of creating physical 3D models of objects using resin or carefully cut and joined pieces of paper. STL files describe only

the surface geometry of a three dimensional object without any representation of color, texture or other common CAD model attributes.

- The IGS (Initial Graphics Exchange Specification) file format is the standard format for transferring three-dimensional models between CAD programs. IGS files can store wireframe models, surface or solid object representations, circuit diagrams, and other objects.
- SLDPRT is the proprietary image file format associated with the SolidWorks brand CAD software. SLDPRT files contain three-dimensional images of one specific part of a product.
- SKP is the CAD drawing format for Google Sketchup, which is a quick, entry-level 3D drawing program.

There are also a small number of Word (.DOC), text (.TXT) or image (.JPG or .BMP) files. A printout of each file is attached to the relevant DS-4076.

As explained further below, each of these files either was previously placed in the public domain or contains only public domain information.

1. Liberator Pistol Data Files

The files for the Liberator Pistol include sixteen STL files for the various parts and components of the pistol, two “read me” text files that explain how to lawfully assemble the pistol, a diagram of a pistol, and a permissive software license. If printed on a 3D printer, the parts could be assembled into a single shot .380 caliber firearm.

2. .22 Electric Data Files

The files for the .22 Electric are two stereolithography (STL) CAD files for models of a barrel and grip for a .22 caliber pistol. If printed, the barrel would be a plastic cylinder with a .22 mm bore and the grip would be a plastic piece with two 5mm diameter holes. If those pieces were printed in plastic and used with an electronic system and firing mechanism, the barrel would be expected to fail upon firing.

3. 125 mm BK-14M High Explosive Anti-Tank Warhead Model Data File

The file is a STL CAD file for a model of a BK-14M high explosive anti-tank warhead without fins. The model, if printed on a 3D printer, would be a solid piece of plastic in the shape of the warhead, but would not be capable of functioning as a warhead.

4. 5.56/.223 Muzzle Brake Data Files

The data files are three different CAD file formats (.IGS, .SLDPRT, and .STL) for a model of a 5.56/.223 muzzle brake. If printed on a 3D printer, the model would be a plastic piece in the shape of the muzzle brake, but would be expected to fail if used with a weapon.

5. Springfield XD-40 Tactical Slide Assembly Data Files

The files are nineteen Computer Aided Design (CAD) data files in the SolidWorks .SLDPRT file format for models of components of a pistol slide for the Springfield XD-40. The

components, if printed on a 3D printer, would be plastic pieces in the shape of the components of the slide assembly, but would be expected to fail if used with a weapon.

6. Sound Moderator – Slip On File

The file is a stereolithography CAD file for a model of a slip-on sound moderator for an air gun. The model, if printed on a 3D printer, would work with an air gun, but would likely melt if used with a firearm.

7. “The Dirty Diane” ½-28 to ¾-16 STP S3600 Oil Filter Silencer Adapter Files

The file is a CAD data file in the SolidWorks .SLDPRT file format for a model of an oil filter silencer adapter that is typically produced in stainless steel. If printed on a 3D printer, this item could be used as a solvent trap adapter, which is used to catch solvents that are used in the process of cleaning a gun. While a metal solvent trap adapter could be used as a silencer, a plastic adapter would likely melt if used with a weapon as a silencer.

8. 12 Gauge to .22 CB Sub-Caliber Insert Files

The files are a SKP CAD file for a model of a sub-caliber insert, two renderings of the sub-caliber insert, and a “read me” text file providing information about the National Firearms Act and the Undetectable Firearms Act. This item, if printed on a 3D printer, would be a plastic cylinder with a .22 bore, and would be expected to fail if used with a weapon.

9. Voltlock Electronic Black Powder System Files

The files are twelve CAD files for models of cylinders of various bores with a touch hole. Eleven of the files are in the STL file format and one is in the IGS format. If those pieces were printed on a 3D printer and used with an electronic ignition, the barrel would be expected to fail.

10. VZ-58 Front Sight Files

The files are a SolidWorks CAD file in the .SLDPRT file format and a rendering of a model of a sight for a VZ-58 rifle. If printed on a 3D printer and used with a weapon, the sight would be expected to fail.

DATA ORIGIN

With the exception of item 1 (Liberator Pistol Data Files), each of these files was provided to Defense Distributed by the creator of the files identified in the DS4076. In addition, as explained below, many of these files were originally posted to www.thingiverse.com or other internet sites, and were freely available to any person with access to the internet.

The Liberator Pistol CAD files were developed by Defense Distributed. The Liberator pistol was designed as a combination of already extant and working files and concepts. The pistol frame, trigger housing, and grip specifications were all taken directly from an AR-15 lower receiver file that is in the public domain. The spring file is taken from a toy car file available on Thingiverse. The hammer relies on striking a common roofing nail, and the barrel is a cylinder bored for .380. The gun functions because of the properties of the .380 cartridge – the brass

casing itself is relied on to act as a breech. The printed and assembled gun is a simple improvised weapon, not as complex as many of the improvised weapons of the 20th century, those available in Army manuals, etc. All of the technologies used to create the Liberator data files are widely available in the public domain.

IDENTICAL & SIMILAR FILES

The Liberator Pistol data files are for an improvised firearm that is similar to and based on numerous items that are available on the internet as well as in various books. The Library of Congress online catalog lists numerous books on gunsmithing, including

- Clyde Baker, Modern gunsmithing; a manual of firearms design, construction, and remodeling for amateurs & professionals (1959)
- John E. Traister, Clyde Baker's Modern gunsmithing : a revision of the classic (1981)
- Frank de Haas, Mr. Single Shot's gunsmithing idea book (1983)
- Roy F. Dunlop, Gunsmithing (1996),
- Franklin Fry, Gunsmithing fundamentals : a guide for professional results (1988),
- James Virgil Howe, The modern gunsmith : a guide for the amateur and professional gunsmith in the design and construction of firearms, with practical suggestions for all who like guns (1982),
- Gérard Métral, A do-it-yourself submachine gun: it's homemade, 9mm, lightweight, durable, and it'll never be on any import ban lists! (1995),
- Jack Mitchell, The Gun digest book of pistolsmithing (1980),
- J. Parrish Stelle, The gunsmith's manual; a complete handbook for the American gunsmith (1883), and
- Patrick Sweeney, Gunsmithing: pistols & revolvers (2009),

among many others. Examples of online sources include:

- <http://www.weaponscombat.com/zip-pipe-and-pen-guns>
- <http://www.infinitearms.com/images2/v/manuals/Misc+Gun+Plans>
- <http://thehomegunsmith.com>
- <http://www.scribd.com/doc/24445441/Pen-Gun-Mk1-Blueprint>
- https://www.google.com/search?q=zip+gun+blueprints&rlz=1C1SKPM_enUS436US489&source=lnms&tbn=isch&sa=X&ei=9t-oUZybJILm8wSx0YHoBg&ved=0CAoQ_AUoAQ&biw=1600&bih=837
- <http://ebookbrowse.com/gu/guns-homemade>

Although DD converted this information into CAD file format, DD does not believe that it created any new technical data for the production of the gun.

A drawing of the 125 BK-14M HEAT (Item 3), including measurements, is currently available on Wikipedia at http://en.wikipedia.org/wiki/File:125mm_BK-14m_HEAT.JPG.

Defense Distributed CJ Requests
June 21, 2013
Page 5

The Sound Moderator CAD file (Item 6) was published on Thingiverse on March 3, 2011 and is still available on that site at <http://www.thingiverse.com/thing:6808>. The VZ-58 Front Sight (Item 10) was also published to Grabcad on December 14, 2012 and is still available on that site at <http://grabcad.com/library/front-sight-for-vz-dot-58-rifle>.

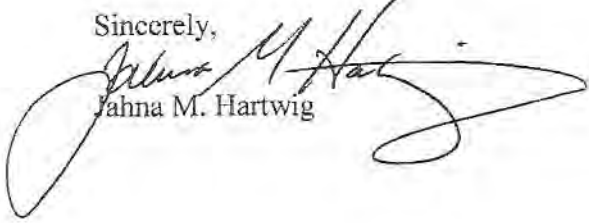
The Oil Filter Silencer Adapter is identical to Solvent Trap Adapters, which are produced by numerous manufacturers and available as commercial products on many websites, including amazon.com. (see http://www.amazon.com/s/ref=nb_sb_noss_1?url=search-alias%3Dautomotive&field-keywords=solvent+trap+adapter&rh=n%3A15684181%2Ck%3Asolvent+trap+adapter.) These items appear to be commercial products that would be subject to the EAR. As such, any related technologies or technical data would also be subject to the EAR.

Examples of CAD files similar to the .22 Electric Pistol (Item 2), Muzzle Brake (Item 4), Slide Assembly (Item 5), and Voltlock Electronic Black Powder System (Item 9) that are currently available on the internet are attached to the relevant DS4076.

As demonstrated above, all of the technical information included in the data files posted to DEFCAD.org was previously available in the public domain. As such, this information is excluded from the definition of "technical data" by 22 C.F.R. § 120.10(a)(5). For these reasons, Defense Distributed respectfully requests that the Department determine that the subject data files posted to DEFCAD.org are not subject to the ITAR.

This submission contains Defense Distributed confidential business information. We respectfully request that the submission be kept confidential. If you need additional information regarding this submission, please contact me at 202-293-8145 or jhartwig@williamsmullen.com.

Sincerely,


Jahna M. Hartwig

EXHIBIT

4

MATTHEW A. GOLDSTEIN, PLLC
1012 14TH STREET, NW, SUITE 820
WASHINGTON, DC 20005

VIA ELECTRONIC FILING

January 2, 2015

PM/DDTC, SA-1, 12th Floor
Office of Defense Trade Controls
Bureau of Political Military Affairs
U.S. Department of State
Washington, D.C. 20522-0012

SUBJECT: Commodity Jurisdiction Request for Ghost Gunner Machine, Plastic Mounting Jig, User Instructions, and Software (Defense Distributed, Inc., PM/DDTC Code M-34702)

Dear Sir or Madam:

Pursuant to Section 120.4 of the International Traffic in Arms Regulations ("ITAR") (22 C.F.R. Sections 120-130), Defense Distributed requests a commodity jurisdiction determination from the Directorate of Defense Trade Controls ("DDTC") on the Ghost Gunner machine (the "Ghost Gunner"), its plastic mounting jig, user instructions, and software for production, operation, and use of the Ghost Gunner.

The Ghost Gunner is an approximately one-foot-cubed black box that uses a drill bit mounted on a head that moves in three dimensions to automatically carve digitally-modeled shapes into polymer, wood or aluminum. It functions as a 3-axis computer-numerically-controlled ("CNC") press that can be used to manufacture parts to firearms controlled under U.S. Munitions List ("USML") Category I. It can also be used to manufacture items that are not controlled under the USML. The machine was designed, developed, and manufactured by Defense Distributed to automatically manufacture publicly available designs with nearly zero user interaction.

As discussed below, the Department of Defense recommended that Defense Distributed submit this commodity jurisdiction request.

Export jurisdiction over the Ghost Gunner, Jig, software, and instructions is uncertain because, although the Department of Commerce Export Administration Regulations ("EAR") maintain a control listing for jigs, fixtures, and other metal-working items "exclusively designed for use in the manufacture of firearms" under Commerce Control List ("CCL") Export Control Number ("ECCN") 2B018.n, there is no corresponding carve-out for these items and related software and technical information otherwise controlled by USML Category I generally; and Category I(i) controls technical data and defense services directly related to firearms, with technical data directly related to the manufacture or production of firearms designated as Significant Military Equipment.

Please note that a letter from Defense Distributed authorizing my law firm to file this request was uploaded with this DS-4076 submission. Please direct any questions and all correspondence related to this request to my office. Communications to me at matthew@goldsteinpllc.com are preferred.

www.GoldsteinPLLC.com

I. BACKGROUND

A. Defense Distributed

Defense Distributed is a Texas corporation, registered with the Department of State under PM/DDTC Code M-34702. The company has developed technical information that can be used to produce, manufacture, and assemble various parts components, accessories, and attachments to firearms controlled under USML Category I. This includes information for the design and production of the Ghost Gunner, software necessary to operate Ghost Gunner, and code that allows production of certain items by the Ghost Gunner.¹

Following notification from DDTC in May 8, 2013, that the agency requires U.S. Government prior approval before publications of otherwise ITAR-controlled technical data into the public domain (Attachment 1), Defense Distributed has submitted requests for U.S. Government clearance of technical data to the Department of Defense Office of Prepublication and Security Review ("DOPSR").² On October 1, 2014, DOPSR returned a Defense Distributed request for clearance of technical information on the Ghost Gunner for public release, stating that commodity jurisdiction over the item was uncertain and recommending that Defense Distributed submit a commodity jurisdiction request. See Attachment 2.

B. The Ghost Gunner

Existing CNC machines are expensive or too inaccurate to manufacture firearms for the casual user. Defense Distributed developed the Ghost Gunner to address this problem by miniaturizing the build envelope to just large enough to mill common firearm receivers, which in turn improves rigidity, reduces material cost and simultaneously relaxes certain design limits, allowing Defense Distributed to sell an inexpensive machine with more than enough accuracy to manufacture firearms.

The first design tested on the Ghost Gunner was for an AR-15 lower receiver and the Ghost Gunner was able to automatically find, align, and mill a so-called "80%" lower receiver, which was not a firearm prior to milling. The Ghost Gunner has since undergone several design revisions to reduce machine chatter, backlash, and jitter, all with the goal of keeping total design cost low.

Photographs of Ghost Gunner are provided at Attachment 3 and rendered images of the machine with the plastic jig are provided at Attachment 4.

¹ This commodity jurisdiction request seeks a determination of the code necessary to operate Ghost Gunner. It does not seek a determination on the various project files specific to production of certain items by the Ghost Gunner.

² In complying with DDTC prepublication review requirements on publication of technical information into the public domain, Defense Distributed does not intend to, nor should it be considered to, waive any defense, claim or right under law.

A schematic drawing for the Ghost Gunner is provided at Attachment 5.

Ghost Gunner form, fit, function, and performance characteristics include the following:

- It uses a compact, powder coated A36 steel frame and thick stainless T-slot rail, with preloaded ball bearings for maximum rigidity. Linear motion is achieved with low-backlash direct-drive ball screws mounted in-line with the cutting surface, thus preventing torsional gantry chatter while machining.
- It incorporates an electronic probe that automatically detects when the machine comes into contact with the work piece, allowing automatic part discovery and alignment. Ghost Gunner requires conductive parts if auto-discovery and alignment are used.
- It can manually machine nonconductive materials, but this requires manual calibration of a part to the machine - following a few simple instructions - as is required with existing CNC machines.
- Its moving parts are entirely sealed from chip debris. All bearings are sealed and contain wipers to prevent foreign contaminate entry. The rails are stainless steel and are factory lubricated, but do require periodic wiping to prolong life. End Mills dull over time and are considered a consumable.
- To contain aluminum chips, it includes a chip collection tray and all moving components are fully enclosed.
- It is capable of manufacturing deep pockets due to its horizontal gantry, which allows gravity to pull chips away from the cutting surface before they can build up and dull the end mill, as is the case on traditional CNC designs.
- It uses industry standard ER-11 collets, and ships with both 1/4" and 5/32" collets.
- It uses a standard IEC power cord and is compatible with any 110/220V circuit. No external power brick is used; the machine is entirely self-contained.
- It has two ports: Power (IEC standard) and USB (Type 'B').
- Its machinable dimensions are 140 x 75 x 60mm (~5.50 x 2.95 x 2.35")
- Its maximum part dimensions are 230 x 90 x 100mm (~9.05 x 3.50 x 3.90")
- Its overall footprint is 330 x 280mm (~13 x 11")
- Its weight is 20kg (~45 pounds)

- Its Spindle Speed is 10,000+ RPM (Final Value TBD)
- Its software requirements are Windows 7 or higher. Mac version TBD

As noted above, Ghost Gunner is capable of manufacturing more than just firearm receivers. With Defense Distributed's open source Physibles Development SDK ("pDev"), designers can distribute files via the company's '.dd' file format, which contains all installation and assembly instructions, any required jig files to hold a part in place (that users can print with a 3D printer), and all machine definitions and code to physically manufacture a particular design. To a casual user, the .dd file is a one-stop solution to manufacturing any aluminum physible that the public can design to fit into the build envelope. Defense Distributed will be developing in and supporting this format.

The .dd file format is itself open source and not constrained to the Ghost Gunner or Defense Distributed; any user can define any existing machine's specific parameters via the machine parameters list. A single file can contain specific code and installation instructions for any number of machines. A user with both a Ghost Gunner and a Tormach P1100 could manufacture a particular .dd file on either machine and manufacture the same physible with zero additional user knowledge, as only the instructions required for a particular machine are revealed to the end user. The .dd file format is a CNC response to 3D printing's universal .stl file format. However, Ghost Gunner will also accept TinyG code from any CAM program.

In operation, users provide the parts for milling. They can then simply plug their computer into the Ghost Gunner, install the Ghost Gunner software, and download any compatible .dd design file. 3D printable jigs are used to hold each part in place as each milling step is performed. For example, milling an eighty percent AR-15 lower receiver requires two jig pieces to secure the lower in place while the trigger pocket is milled, and then two more jig pieces are installed to drill the trigger pinholes. As most eighty percent firearms require deep pocket milling, Ghost Gunner's mounting table is parallel to the end mill shaft. This orientation maximizes 3D printed jig strength, minimizes jig complexity, and mechanically aligns the part to the machine upon insertion into the Maker Slide-patterned, Open Source T Slot stainless rails.

Defense Distributed expects its typical order fulfillment will contain the fully assembled Ghost Gunner CNC, plastic mounting jig designed to secure 80% AR-15 receivers, operating software and instructions. Defense Distributed also intends to place instructions and computer code needed to build and use Ghost Gunner into the public domain as Open Source technology.

Block 13 ("Sales information") is not provided with this request because the Ghost Gunner is still in development as Defense Distributed awaits arrival of various production pieces and continues to make any required changes to the product. As such, the company has not yet delivered any machines (i.e., no completed sales). However, the company has accepted 469 pre-orders and 413 advance deposits from prospective purchasers. Each of these orders, except for one, are intended for domestic sale. In addition, consistent with U.S. law, final sales will carry conditions that limit purchases to private use (i.e., not for commercial or military use).

C. User Instructions and Operating Software for the Ghost Gunner

The current draft User Instructions for the Ghost Gunner accompanies this commodity jurisdiction request at Attachment 6. It contains information on how to attach a “80%” lower receiver to Ghost Gunner, such that Ghost Gunner can mill and drill all required holes to transform the lower receiver into a firearm. Ghost Gunner presents numerous User Instructions, User Graphics, and User Selections to the operator. Ghost Gunner performs work via Calibration Code and Milling Code. Ghost Gunner also assists the user in creating 3D printable Jigs, if needed.

The software necessary to produce and operate the Ghost Gunner includes AutoDesk Inventor and a simple executable application that can interpret CNC part files and TinyG code. Additional information detailing the purpose, function, and capability of the software, as requested by DDTC’s DS-4076 Commodity Jurisdiction (CJ) Guidance for Software, accompanies this commodity jurisdiction request at Attachment 7.

II. COMMODITY JURISDICTION STANDARD

The standard applicable to Department of State and other agency considerations of commodity jurisdiction is set forth at ITAR Section 120.3. ITAR Subsection 120.3(a) extends Department of State jurisdiction to any item that meets the criteria of a defense article described on the USML or that provides equivalent performance capabilities; and ITAR Section 120.3(b) provides that a specific article not presently described on the USML shall be determined in the future as a defense article if it provides a critical military or intelligence advantage.

A. Relevant USML Control Listings

Subparagraph (h) to USML Category I controls components, parts, accessories, and attachments for firearms to .50 caliber inclusive. The Ghost Gunner does not meet the Category I(h) criteria because it is not a component or part to a firearm. Rather, it is a machine that can be used for the manufacture of such articles.

Subparagraph (i) to USML Category I controls technical data, to include “software” as defined at Section 120.45(f), and defense services directly related to the firearms and components, parts, accessories, and attachments for firearms to .50 caliber inclusive. Technical data directly related to the manufacture or production of firearms controlled in Category I is designated as Significant Military Equipment.

The USML does not contain a control listing that describes items used for the manufacture of firearms. Instead, that listing is contained on the EAR Commerce Control List (“CCL”) entry for ECCN 2B018.n, which controls “Jigs and fixtures and other metal-working implements or “accessories” of the kinds exclusively designed for use in the manufacture of firearms. ECCN 2D018 controls software” for the “development”, “production” or “use” of equipment controlled by 2B018; and ECCN 2E018, in turn, controls “Technology” for the “use” of equipment controlled by 2B018.

The scope of the CCL controls on firearms manufacturing equipment and technology is unclear because the EAR only controls items not described on the USML and Category I does not contain any carve-out from ITAR control for software or technology controlled under ECCNs 2D018 and 2E018. To the contrary, if literally applied, USML Category I(i) treats such technical information as Significant Military Equipment.

Because there is no specific carve-out in Category I or elsewhere in the USML for software or technology controlled by 2D018 and 2E018, it is very difficult to distinguish between technical data for the manufacture or production of firearms controlled in Category I and technology for the development, production, and use of equipment used to manufacture firearms controlled at 2D018 and 2E018. This is a primary concern of the present commodity jurisdiction request.

Nevertheless, EAR control is consistent with U.S. Implementation of Wassenaar Controls. Specifically, ECCNs 2B018, ECCN 2E018, and 2B018 are Wassenaar Arrangement-based controls, subject to the National Security reason for control and which correspond to Category 2 of the Wassenaar Arrangement List of Dual-Use Items. In fact, 2B018 is titled, "Equipment on the Wassenaar Arrangement Munitions List."

Although relevant text of the ITAR and EAR control listings lack clarity, it appears that the U.S. Government decided to implement export controls on firearms manufacturing equipment and associated technical information in the EAR when it first implemented the Wassenaar Arrangement controls for such items. Accordingly, Defense Distributed believes that the Ghost Gunner does not meet criteria of a defense article described on the USML and that it does not provide equivalent performance capabilities to an article described on the USML.

Defense Distributed further notes that the DDTC should consider amending USML Category I to provide an express carve-out for EAR items controlled under ECCNs 2B018.n, ECCN 2E018, and 2B018. Alternatively, if DDTC intends to control firearms manufacturing equipment under the USML, it should make this clear in the regulations. Towards this end, any determination on the instant request that imposes ITAR control should be widely disseminated and shared with the firearms manufacturing industry.

B. Ghost Gunner Does Not Provide a Critical Military or Intelligence Advantage.

As noted above, ITAR Section 120.3(b) provides that a specific article not presently described on the USML shall be determined in the future as a defense article if it provides a critical military or intelligence advantage.

The function and performance of the Ghost Gunner does not provide a critical military or intelligence advantage. Rather, it is essentially a jig press based on a simple design that is easily replicated by any skilled machinist. In fact, the Ghost Gunner can be produced by persons with no formal engineering background.

In addition, Ghost Gunner builds on technology readily available in the Open Source community, including the gshield 3 axis motion hardware (<http://synthetos.myshopify.com/products/gshield-v5>), the grbl g-code parser and motion controller (<https://github.com/grbl/grbl>), and the Arduino microcontroller (<http://arduino.cc>).

Further, instructions and/or electronic files for production of jig presses with similar form, fit, and function to the Ghost Gunner are publicly available for download at a variety of web addresses, to include the following:

<http://aresarmor.com/store/Item/Polymer-80-Black>
<http://www.thingiverse.com/thing:160266>
https://github.com/DefiantCad/defcad-repo/tree/master/Rifles/AR-15_80_percent_lower_v5-shadowfall/AR-15_80_percent_Lower_Drill_Jig_v1-Shadowfall
<http://www.advancedrifles.com/3d-printed-jig-version-2-0/>
<http://www.80percentarms.com/products/80-ar-15-easy-jig>
<http://www.sierranevadaarms.com/jig.pdf>
<http://www.rockethub.com/projects/24384-80-lower-receiver-ar15-ar10-rudius-1911>

III. CONCLUSION

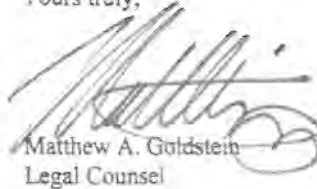
Considering the apparent intent of the U.S. Government in implementing relevant Wassenaar Arrangement controls in the EAR, Defense Distributed believes that the Ghost Gunner does not meet the criteria of an article described on the USML. In addition, the Ghost Gunner does not provide a critical military or intelligence advantage. Accordingly, Defense Distributed respectfully requests that the Department of State issue a commodity jurisdiction determination stating that the Ghost Gunner, its plastic mounting jig, operating software, and production and operation instructions do not meet the criteria of ITAR 120.3 and are subject to Department of Commerce jurisdiction under the EAR.

Defense Distributed authorizes the release for general publication of the information contained in Block 5 of the DS-4076 Form. However, other information in this request and documents submitted with Defense Distributed's DS-4076 Submission contain sensitive business information that is proprietary, confidential, and exempt from disclosure under the Freedom of Information Act, 5 U.S.C. Section 552, and is also protected under the Trade Secrets Act, 18 U.S.C. Section 1905. Accordingly, pursuant to ITAR Section 130.15, Defense Distributed requests that information in this submission other than that contained in Block 5 be withheld in the event of a request for its disclosure.

Commodity Jurisdiction Request
January 2, 2015
Page 8 of 9

Thank you for your prompt attention to this matter and please contact me at 202-550-0040 or at matthew@goldsteinpllc.com if any additional information is needed.

Yours truly,


Matthew A. Goldstein
Legal Counsel

COMPANY CERTIFICATION:

Cody Wilson, the Principal of Defense Distributed, certifies that he is the duly authorized representative of Defense Distributed; and that in such capacity, he certifies that he has carefully read the foregoing Commodity Jurisdiction request; and that the contents of the request are true and correct to the best of his knowledge, information and belief after reasonable inquiry into the matters discussed.


Signature

1/2/2015
Date

ATTACHMENTS TO LETTER OF EXPLANATION:

- | | |
|--------------|--|
| Attachment 1 | May 8, 2013 DDTC Letter to Defense Distributed |
| Attachment 2 | October 1, 2014 DOPSR Letter to Defense Distributed |
| Attachment 3 | Photographs of Ghost Gunner Machine |
| Attachment 4 | Rendered Images of Ghost Gunner Machine |
| Attachment 5 | Ghost Gunner Schematics |
| Attachment 6 | Ghost Gunner User Instructions |
| Attachment 7 | Answers to DS-4076 Commodity Jurisdiction (CJ) Guidance for Software |

www.GoldsteinPLLC.com

Commodity Jurisdiction Request
January 2, 2015
Page 9 of 9

OTHER ATTACHMENTS INCLUDED WITH DS-4076 SUBMISSION:

DD_DS4076.pdf

DD_Attorney_Authorization_Letter_Block_2-1.pdf

[Instant document] DD_Cover_Ltr_Block_6-1.pdf

DD_Certification_Block_19-1.pdf

EXHIBIT

5



United States Department of State

Bureau of Political-Military Affairs
Directorate of Defense Trade Controls

Washington, D.C. 20522-0112

In Reply refer to
DDTC Case CJ 1083-14 (RE-ISSUE)

APR 15 2015

YOUR SUBMISSION DATED: January 2, 2015

COMMODITY JURISDICTION DETERMINATION FOR: **Ghost Gunner Machine, Plastic Mounting Jig, User Instructions, and Software**

The product described in your submission is a one cubic foot box that functions as a 3-axis, computer-numerically-controlled (CNC) press capable of automatically milling parts out of various materials through software designs.

A technical review of your commodity jurisdiction (CJ) request has been concluded by the requisite agencies of the United States Government. A split jurisdiction determination of this request has been determined, as follows:

The Department of State has determined that the **Ghost Gunner, its plastic mounting jig, operating software, and production and operation instructions are not subject to the jurisdiction of the Department of State.** However, export may require authorization from the Department of Commerce (DOC). Please consult the DOC Office of Exporter Services at (202) 482-4811 to make a Classification Request (CCATS) and satisfy other applicable requirements prior to export.

The Department of State has determined that the **project files, data files, or any form of technical data for producing a defense article, including an 80% AR-15 lower receiver, are subject to the jurisdiction of the Department of State in accordance with the International Traffic in Arms Regulations (ITAR) (22 CFR 120 through 130).** They are

Continued on Page Two

Cody R. Wilson
Defense Distributed, Inc.
1101 W 34th Street, #340
Austin, TX 78705
crw@defdist.org

Page Two

In Reply refer to
DDTC Case CJ 1083-14

designated as technical data under Category I(i) of the United States Munitions List (USML). A license or other approval is required pursuant to the ITAR prior to any export or temporary import.

Should you not agree with this determination and have additional facts not included in the original submission, you may submit a new CJ request. If you do not agree with this determination and have no additional facts to present, you may request that this determination be reviewed by the Deputy Assistant Secretary of State for Defense Trade Controls.

Should you require further assistance on this matter, please contact Samuel Harmon at (202) 663-2811 or HarmonSC@state.gov.

Sincerely,



C. Edward Peartree

Director

Office of Defense Trade Controls Policy

Cc: Matthew A. Goldstein
1012 14th Street, NW, Suite 620
Washington, DC 20005
matthew@goldsteinpllc.com

EXHIBIT

6



United States Department of State

*Bureau of Political-Military Affairs
Directorate of Defense Trade Controls*

Washington, D.C. 20522-0112

In Reply refer to
DDTC Cases CJ 651-13 through 660-13

JUN 04 2013

YOUR SUBMISSION DATED: June 21, 2013

COMMODITY JURISDICTION DETERMINATIONS FOR: Liberator Pistol Data Files, .22 Electric Data Files, 125 mm BK-14M High Explosive Anti-Tank Warhead Model Data File, 5.56/.223 Muzzle Brake Data Files, Springfield XD-40 Tactical Slide Assembly Data Files, Sound Moderator - Slip On Data File, "The Dirty Diane" Oil Filter Silencer Adapter Data File, 12 Gauge to .22 CB Sub-Caliber Insert Data Files, Voltlock Electronic Black Powder System Data Files, and VZ-58 Front Sight Data Files

The data described in your submission are Computer Aided Design (CAD) data files that can be used in a 3D printer to produce physical models of the associated item.

A technical review of your commodity jurisdiction (CJ) request has been concluded by requisite agencies of the United States Government. The findings of that technical review are:

The Department of State has determined that the **125 mm BK-14M High Explosive Anti-Tank Warhead Model Data File, Sound Moderator - Slip On Data File, and "The Dirty Diane" Oil Filter Silencer Adapter Data File** are not subject to the jurisdiction of the Department of State. The Department of Commerce (DOC) advises that these items are classified as EAR99. Please consult the DOC Office of Exporter Services at (202) 482-4811 to satisfy applicable requirements prior to export.

The Department of State has determined that the **Voltlock Electronic Black Powder System Data Files** are not subject to the jurisdiction of the

Continued on Page Two

Cody R. Wilson
Defense Distributed
711 W. 32nd Street, Apt. 115
Austin, TX 78705
crw@defdist.org

Page Two

In Reply refer to
DDTC Cases CJ 651-13 through 660-13

Department of State. However, export may require authorization from the Department of Commerce (DOC). Please consult the DOC Office of Exporter Services at (202) 482-4811 to make a Classification Request (CCATS) and satisfy other applicable requirements prior to export.

The Department of State has determined that the **Liberator Pistol Data Files, .22 Electric Data Files, 5.56/.223 Muzzle Brake Data Files, Springfield XD-40 Tactical Slide Assembly Data Files, 12 Gauge to .22 CB Sub-Caliber Insert Data Files (except for "read me" text file), and VZ-58 Front Sight Data Files** are subject to the jurisdiction of the Department of State in accordance with the **International Traffic in Arms Regulations (ITAR) (22 CFR 120 through 130)**. They are designated as technical data under Category I(i) of the United States Munitions List (USML) pursuant to §120.10 of the ITAR. A license or other approval is required pursuant to the ITAR prior to any export or temporary import.

Should you not concur with this determination and have additional facts not included in the original submission, you may submit a new CJ request. If you do not concur with this determination and have no additional facts to present, then you may request that this determination be reviewed by the Deputy Assistant Secretary of State for Defense Trade Controls.

Should you require further assistance on this matter, please contact Sam Harmon at (202) 663-2811 or HarmonSC@state.gov.

Sincerely,



C. Edward Peartree

Director

Office of Defense Trade Controls Policy

Cc: Matthew A. Goldstein
1012 14th Street, NW, Suite 620
Washington, DC 20005
matthew@goldsteinpllc.com

EXHIBIT

7

hearing," which are conducted pursuant to the provisions of 5 U.S.C. 556 and 557. The CSA sets forth the criteria for scheduling a drug or other substance and for removing a drug or substance from the schedules of controlled substances. Such actions are exempt from review by the Office of Management and Budget (OMB) pursuant to section 3(d)(1) of Executive Order 12866 and the principles reaffirmed in Executive Order 13563.

Executive Order 12988

This regulation meets the applicable standards set forth in sections 3(a) and 3(b)(2) of Executive Order 12988 Civil Justice Reform to eliminate drafting errors and ambiguity, minimize litigation, provide a clear legal standard for affected conduct, and promote simplification and burden reduction.

Executive Order 13132

This rulemaking does not have federalism implications warranting the application of Executive Order 13132. The rule does not have substantial direct effects on the States, on the relationship between the Federal Government and the States, or the distribution of power and responsibilities among the various levels of government.

Executive Order 13175

This rule does not have tribal implications warranting the application of Executive Order 13175. This rule does not have substantial direct effects on one or more Indian tribes, on the relationship between the Federal Government and Indian tribes, or on the distribution of power and responsibilities between the Federal Government and Indian tribes.

Regulatory Flexibility Act

The Administrator, in accordance with the Regulatory Flexibility Act (5 U.S.C. 601–612) (RFA), has reviewed this proposed rule and by approving it certifies that it will not have a significant economic impact on a substantial number of small entities. The purpose of this rule is to remove [123I]ioflupane from the list of schedules of the CSA. This action will remove regulatory controls and administrative, civil, and criminal sanctions applicable to controlled substances for handlers and proposed handlers of [123I]ioflupane. Accordingly, it has the potential for some economic impact in the form of cost savings.

If finalized, the proposed rule will affect all persons who would handle, or propose to handle, [123I]ioflupane. Due to the wide variety of unidentifiable and

unquantifiable variables that potentially could influence the distribution and administration rates of new molecular entities, the DEA is unable to determine the number of entities and small entities which might handle [123I]ioflupane.

Although the DEA does not have a reliable basis to estimate the number of affected entities and quantify the economic impact of this proposed rule, a qualitative analysis indicates that, if finalized, this rule is likely to result in some cost savings for the healthcare industry. The affected entities will continue to meet existing Federal and/or state requirements applicable to those who handle radiopharmaceutical substances, including licensure, security, recordkeeping, and reporting requirements, which in many cases are more stringent than the DEA's requirements. However, the DEA estimates cost savings will be realized from the removal of the administrative, civil, and criminal sanctions for those entities handling or proposing to handle [123I]ioflupane, in the form of saved registration fees, and the elimination of additional physical security, recordkeeping, and reporting requirements.

Because of these facts, this rule will not result in a significant economic impact on a substantial number of small entities.

Unfunded Mandates Reform Act of 1995

On the basis of information contained in the "Regulatory Flexibility Act" section above, the DEA has determined and certifies pursuant to the Unfunded Mandates Reform Act of 1995 (UMRA), 2 U.S.C. 1501 *et seq.*, that this action would not result in any federal mandate that may result "in the expenditure by State, local, and tribal governments, in the aggregate, or by the private sector, of \$100,000,000 or more (adjusted for inflation) in any one year * * *." Therefore, neither a Small Government Agency Plan nor any other action is required under provisions of UMRA.

Paperwork Reduction Act

This action does not impose a new collection of information requirement under the Paperwork Reduction Act, 44 U.S.C. 3501–3521. This action would not impose recordkeeping or reporting requirements on State or local governments, individuals, businesses, or organizations. An agency may not conduct or sponsor, and a person is not required to respond to, a collection of information unless it displays a currently valid OMB control number.

List of Subjects in 21 CFR part 1308

Administrative practice and procedure, Drug traffic control, Reporting and recordkeeping requirements.

For the reasons set out above, 21 CFR part 1308 is proposed to be amended to read as follows:

PART 1308—SCHEDULES OF CONTROLLED SUBSTANCES

■ 1. The authority citation for 21 CFR part 1308 continues to read as follows:

Authority: 21 U.S.C. 811, 812, 871(b), unless otherwise noted.

■ 2. In § 1308.12, revise paragraph (b)(4) to read as follows:

§ 1308.12 Schedule II.

* * * * *

(b) * * *

(4) Coca leaves (9040) and any salt, compound, derivative or preparation of coca leaves (including cocaine (9041) and ecgonine (9180) and their salts, isomers, derivatives and salts of isomers and derivatives), and any salt, compound, derivative, or preparation thereof which is chemically equivalent or identical with any of these substances, except that the substances shall not include:

- (i) Decocainized coca leaves or extraction of coca leaves, which extractions do not contain cocaine or ecgonine; or
- (ii) [123I]ioflupane.

* * * * *

Dated: May 6, 2015.

Michele M. Leonhart,
Administrator.

[FR Doc. 2015–13455 Filed 6–2–15; 8:45 am]

BILLING CODE 4410–09–P

DEPARTMENT OF STATE

22 CFR Parts 120, 123, 125, and 127

[Public Notice 9149]

RIN 1400–AD70

International Traffic in Arms: Revisions to Definitions of Defense Services, Technical Data, and Public Domain; Definition of Product of Fundamental Research; Electronic Transmission and Storage of Technical Data; and Related Definitions

AGENCY: Department of State.

ACTION: Proposed rule.

SUMMARY: As part of the President's Export Control Reform (ECR) initiative, the Department of State proposes to amend the International Traffic in Arms

Regulations (ITAR) to update the definitions of "defense article," "defense services," "technical data," "public domain," "export," and "reexport or retransfer" in order to clarify the scope of activities and information that are covered within these definitions and harmonize the definitions with the Export Administration Regulations (EAR), to the extent appropriate. Additionally, the Department proposes to create definitions of "required," "technical data that arises during, or results from, fundamental research," "release," "retransfer," and "activities that are not exports, reexports, or retransfers" in order to clarify and support the interpretation of the revised definitions that are proposed in this rulemaking. The Department proposes to create new sections detailing the scope of licenses, unauthorized releases of information, and the "release" of secured information, and revises the sections on "exports" of "technical data" to U.S. persons abroad. Finally, the Department proposes to address the electronic transmission and storage of unclassified "technical data" via foreign communications infrastructure. This rulemaking proposes that the electronic transmission of unclassified "technical data" abroad is not an "export," provided that the data is sufficiently secured to prevent access by foreign persons. Additionally, this proposed rule would allow for the electronic storage of unclassified "technical data" abroad, provided that the data is secured to prevent access by parties unauthorized to access such data. The revisions contained in this proposed rule are part of the Department of State's retrospective plan under Executive Order 13563 first submitted on August 17, 2011.

DATES: The Department of State will accept comments on this proposed rule until August 3, 2015.

ADDRESSES: Interested parties may submit comments within 60 days of the date of publication by one of the following methods:

- **Email:** DDTCTPublicComments@state.gov with the subject line, "ITAR Amendment—Revisions to Definitions; Data Transmission and Storage."
- **Internet:** At www.regulations.gov, search for this notice by using this rule's RIN (1400-AD70).

Comments received after that date may be considered, but consideration cannot be assured. Those submitting comments should not include any personally identifying information they do not desire to be made public or information for which a claim of

confidentiality is asserted because those comments and/or transmittal emails will be made available for public inspection and copying after the close of the comment period via the Directorate of Defense Trade Controls Web site at www.pmdtdc.state.gov. Parties who wish to comment anonymously may do so by submitting their comments via www.regulations.gov, leaving the fields that would identify the commenter blank and including no identifying information in the comment itself. Comments submitted via www.regulations.gov are immediately available for public inspection.

FOR FURTHER INFORMATION CONTACT: Mr. C. Edward Peartree, Director, Office of Defense Trade Controls Policy, Department of State, telephone (202) 663-1282; email DDTCResponseTeam@state.gov. ATTN: ITAR Amendment—Revisions to Definitions; Data Transmission and Storage. The Department of State's full retrospective plan can be accessed at <http://www.state.gov/documents/organization/181028.pdf>.

SUPPLEMENTARY INFORMATION: The Directorate of Defense Trade Controls (DDTC), U.S. Department of State, administers the International Traffic in Arms Regulations (ITAR) (22 CFR parts 120 through 130). The items subject to the jurisdiction of the ITAR, *i.e.*, "defense articles" and "defense services," are identified on the ITAR's U.S. Munitions List (USML) (22 CFR 121.1). With few exceptions, items not subject to the export control jurisdiction of the ITAR are subject to the jurisdiction of the Export Administration Regulations ("EAR," 15 CFR parts 730 through 774, which includes the Commerce Control List (CCL) in Supplement No. 1 to part 774), administered by the Bureau of Industry and Security (BIS), U.S. Department of Commerce. Both the ITAR and the EAR impose license requirements on exports and reexports. Items not subject to the ITAR or to the exclusive licensing jurisdiction of any other set of regulations are subject to the EAR.

BIS is concurrently publishing comparable proposed amendments (BIS companion rule) to the definitions of "technology," "required," "peculiarly responsible," "published," results of "fundamental research," "export," "reexport," "release," and "transfer (in-country)" in the EAR. A side-by-side comparison on the regulatory text proposed by both Departments is available on both agencies' Web sites: www.pmdtdc.state.gov and www.bis.doc.gov.

1. Revised Definition of Defense Article

The Department proposes to revise the definition of "defense article" to clarify the scope of the definition. The current text of § 120.6 is made into a new paragraph (a), into which software is added to the list of things that are a "defense article" because software is being removed from the definition of "technical data." This is not a substantive change.

A new § 120.6(b) is added to list those items that the Department has determined should not be a "defense article," even though they would otherwise meet the definition of "defense article." All the items described were formerly excluded from the definition of "technical data" in § 120.10. These items are declared to be not subject to the ITAR to parallel the EAR concept of "not subject to the EAR" as part of the effort to harmonize the ITAR and the EAR. This does not constitute a change in policy regarding these items or the scope of items that are defense articles.

2. Revised Definition of Technical Data

The Department proposes to revise the definition of "technical data" in ITAR § 120.10 in order to update and clarify the scope of information that may be captured within the definition. Paragraph (a)(1) of the revised definition defines "technical data" as information "required" for the "development," "production," operation, installation, maintenance, repair, overhaul, or refurbishing of a "defense article," which harmonizes with the definition of "technology" in the EAR and the Wassenaar Arrangement. This is not a change in the scope of the definition, and additional words describing activities that were in the prior definition are included in parentheses to assist exporters.

Paragraph (a)(1) also sets forth a broader range of examples of formats that "technical data" may take, such as diagrams, models, formulae, tables, engineering designs and specifications, computer-aided design files, manuals or documentation, or electronic media, that may constitute "technical data." Additionally, the revised definition includes certain conforming changes intended to reflect the revised and newly added defined terms proposed elsewhere in this rule.

The proposed revised definition also includes a note clarifying that the modification of the design of an existing item creates a new item and that the "technical data" for the modification is "technical data" for the new item.

Paragraph (a)(2) of the revised definition defines "technical data" as

also including information that is enumerated on the USML. This will be “technical data” that is positively described, as opposed to “technical data” described in the standard catch-all “technical data” control for all “technical data” directly related to a “defense article” described in the relevant category. The Department intends to enumerate certain controlled “technical data” as it continues to move the USML toward a more positive control list.

Paragraph (a)(3) of the revised definition defines “technical data” as also including classified information that is for the “development,” “production,” operation, installation, maintenance, repair, overhaul, or refurbishing of a “defense article” or a 600 series item subject to the EAR. Paragraph (a)(5) of the revised definition defines “technical data” as also including information to access secured “technical data” in clear text, such as decryption keys, passwords, or network access codes. In support of the latter change, the Department also proposes to add a new provision to the list of violations in § 127.1(b)(4) to state that any disclosure of these decryption keys or passwords that results in the unauthorized disclosure of the “technical data” or software secured by the encryption key or password is a violation and will constitute a violation to the same extent as the “export” of the secured information. For example, the “release” of a decryption key may result in the unauthorized disclosure of multiple files containing “technical data” hosted abroad and could therefore constitute a violation of the ITAR for each piece of “technical data” on that server.

Paragraph (b) of the revised definition of “technical data” excludes non-proprietary general system descriptions, information on basic function or purpose of an item, and telemetry data as defined in Note 3 to USML Category XV(f) (§ 121.1). Items formerly identified in this paragraph, principles taught in schools and “public domain” information, have been moved to the new ITAR § 120.6(b).

The proposed definition removes software from the definition of “technical data.” Specific and catch-all controls on software will be added elsewhere throughout the ITAR as warranted, as it will now be defined as a separate type of “defense article.”

3. Proposed Definition of Required

The Department proposes a definition of “required” in a new § 120.46. “Required” is used in the definition of “technical data” and has, to this point,

been an undefined term in the ITAR. The word is also used in the controls on technology in both the EAR and the Wassenaar Arrangement, as a defined term, which the Department is now proposing to adopt:

... [O]nly that portion of [technical data] that is peculiarly responsible for achieving or exceeding the controlled performance levels, characteristics, or functions. Such required [technical data] may be shared by different products.

The proposed definition of “required” contains three notes. These notes explain how the definition is to be applied.

Note 1 provides that the definition explicitly includes information for meeting not only controlled performance levels, but also characteristics and functions. All items described on the USML are identified by a characteristic or function. Additionally, some descriptions include a performance level. As an example, USML Category VIII(a)(1) controls aircraft that are “bombers” and contains no performance level. The characteristic of the aircraft that is controlled is that it is a bomber, and therefore, any “technical data” peculiar to making an aircraft a bomber is “required.”

Note 2 states that, with the exception of “technical data” specifically enumerated on the USML, the jurisdictional status of unclassified “technical data” is the same as that of the commodity to which it is directly related. Specifically, it explains that “technical data” for a part or component of a “defense article” is directly related to that part or component, and if the part or component is subject to the EAR, so is the “technical data.”

Note 3 establishes a test for determining if information is peculiarly responsible for meeting or achieving the controlled performance levels, characteristics or functions of a “defense article.” It uses the same catch-and-release concept that the Department implemented in the definition of “specially designed.” It has a similarly broad catch of all information used in or for use in the “development,” “production,” operation, installation, maintenance, repair, overhaul, or refurbishing of a “defense article.” It has four releases that mirror the “specially designed” releases, and one reserved paragraph for information that the Department determines is generally insignificant. The first release is for information identified in a commodity jurisdiction determination. The second release is reserved. The third release is for information that is identical to information used in a non-defense

article that is in “production,” and not otherwise enumerated on the ITAR. The fourth release is for information that was developed with knowledge that it is for both a “defense article” and a non-defense article. The fifth release is information that was developed for general purpose commodities.

In the companion rule, BIS proposes to make Note 3 into a stand-alone definition for “peculiarly responsible” as it has application outside of the definition of “required.” The substance of Note 3 and the BIS definition of “peculiarly responsible” are identical. DDTTC asks for comments on the placement of this concept.

4. Proposed Definitions of Development and Production

The Department proposes to add § 120.47 for the definition of “development” and § 120.48 for the definition of “production.” These definitions are currently in Notes 1 and 2 to paragraph (b)(3) in § 120.41, the definition of “specially designed.” Because “technical data” is now defined, in part, as information “required” for the “development” or “production” of a “defense article,” and these words are now used in the definition of a “defense service,” it is appropriate to define these terms. The adoption of these definitions is also done for the purpose of harmonization because these definitions are also used in the EAR and by the Wassenaar Arrangement.

5. Revised Definition of Public Domain

The Department proposes to revise the definition of “public domain” in ITAR § 120.11 in order to simplify, update, and introduce greater versatility into the definition. The existing version of ITAR § 120.11 relies on an enumerated list of circumstances through which “public domain” information might be published. The Department believes that this definition is unnecessarily limiting in scope and insufficiently flexible with respect to the continually evolving array of media, whether physical or electronic, through which information may be disseminated.

The proposed definition is intended to identify the characteristics that are common to all of the enumerated forms of publication identified in the current rule—with the exception of ITAR § 120.11(a)(8), which is addressed in a new definition for “technical data that arises during, or results from, fundamental research”—and to present those common characteristics in a streamlined definition that does not require enumerated identification

within the ITAR of every current or future qualifying publication scenario. Additionally, the proposed definition incorporates phrases such as “generally accessible” and “without restriction upon its further dissemination” in order to better align the definition found in the EAR and more closely aligned with the definition in the Wassenaar Arrangement control lists.

The proposed definition requires that information be made available to the public without restrictions on its further dissemination. Any information that meets this definition is “public domain.” The definition also retains an exemplary list of information that has been made available to the public without restriction and would be considered “public domain.” These include magazines, periodicals and other publications available as subscriptions, publications contained in libraries, information made available at a public conference, meeting, seminar, trade show, or exhibition, and information posted on public Web sites. The final example deems information that is submitted to co-authors, editors, or reviewers or conference organizers for review for publication to be “public domain,” even prior to actual publication. The relevant restrictions do not include copyright protections or generic property rights in the underlying physical medium.

Paragraph (b) of the revised definition explicitly sets forth the Department’s requirement of authorization to release information into the “public domain.” Prior to making available “technical data” or software subject to the ITAR, the U.S. government must approve the release through one of the following: (1) The Department; (2) the Department of Defense’s Office of Security Review; (3) a relevant U.S. government contracting authority with authority to allow the “technical data” or software to be made available to the public, if one exists; or (4) another U.S. government official with authority to allow the “technical data” or software to be made available to the public.

The requirements of paragraph (b) are not new. Rather, they are a more explicit statement of the ITAR’s requirement that one must seek and receive a license or other authorization from the Department or other cognizant U.S. government authority to release ITAR controlled “technical data,” as defined in § 120.10. A release of “technical data” may occur by disseminating “technical data” at a public conference or trade show, publishing “technical data” in a book or journal article, or posting “technical data” to the Internet. This proposed provision will enhance

compliance with the ITAR by clarifying that “technical data” may not be made available to the public without authorization. Persons who intend to discuss “technical data” at a conference or trade show, or to publish it, must ensure that they obtain the appropriate authorization.

Information that is excluded from the definition of “defense article” in the new § 120.6(b) is not “technical data” and therefore does not require authorization prior to release into the “public domain.” This includes information that arises during or results from “fundamental research,” as described in the new § 120.49; general scientific, mathematical, or engineering principles commonly taught in schools, and information that is contained in patents.

The Department also proposes to add a new provision to § 127.1 in paragraph (a)(6) to state explicitly that the further dissemination of “technical data” or software that was made available to the public without authorization is a violation of the ITAR, if, and only if, it is done with knowledge that the “technical data” or software was made publicly available without an authorization described in ITAR § 120.11(b)(2). Dissemination of publicly available “technical data” or software is not an export-controlled event, and does not require authorization from the Department, in the absence of knowledge that it was made publicly available without authorization.

“Technical data” and software that is made publicly available without proper authorization remains “technical data” or software and therefore remains subject to the ITAR. As such, the U.S. government may advise a person that the original release of the “technical data” or software was unauthorized and put that person on notice that further dissemination would violate the ITAR.

6. Proposed Definition of Technical Data That Arises During, or Results From, Fundamental Research

The Department proposes to move “fundamental research” from the definition of “public domain” in ITAR § 120.11(a)(8) and define “technical data that arises during, or results from, fundamental research” in a new ITAR § 120.49. The Department believes that information that arises during, or results from fundamental research is conceptually distinguishable from the information that would be captured in the revised definition of “public domain” that is proposed in this rule. Accordingly, the Department proposes to address this concept with its own definition. The new definition of

“technical data that arises during, or results from, fundamental research” is consistent with the prior ITAR § 120.11(a)(8), except that the Department has expanded the scope of eligible research to include research that is funded, in whole or in part, by the U.S. government.

7. Revised Definition of Export

The Department proposes to revise the definition of “export” in ITAR § 120.17 to better align with the EAR’s revised definition of the term and to remove activities associated with a defense article’s further movement or release outside the United States, which will now fall within the definition of “reexport” in § 120.19. The definition is revised to explicitly identify that ITAR §§ 126.16 and 126.17 (exemptions pursuant to the Australia and UK Defense Trade Cooperation Treaties) have their own definitions of “export,” which apply exclusively to those exemptions. It also explicitly references the new § 120.49, “Activities that are Not Exports, Reexports, or Retransfers,” which excludes from ITAR control certain transactions identified therein.

Paragraph (a)(1) is revised to parallel the definition of “export” in proposed paragraph (a)(1) of § 734.13 of the EAR. Although the wording has changed, the scope of the control is the same. The provision excepting travel outside of the United States by persons whose personal knowledge includes “technical data” is removed, but the central concept is unchanged. The “release” of “technical data” to a foreign person while in the United States or while travelling remains a controlled event.

Paragraph (a)(2) includes the control listed in the current § 120.17(a)(4) (transfer of technical data to a foreign person). The proposed revisions replace the word “disclosing” with “releasing,” and the paragraph is otherwise revised to parallel proposed paragraph (a)(2) of § 734.13 of the EAR. “Release” is a newly defined concept in § 120.50 that encompasses the previously undefined term “disclose.”

Paragraph (a)(3) includes the control listed in the current § 120.17(a)(2) (transfer of registration, control, or ownership to a foreign person of an aircraft, vessel, or satellite). It is revised to parallel proposed paragraph (a)(3) of § 734.13 of the EAR.

Paragraph (a)(4) includes the control listed in the current § 120.17(a)(3) (transfer in the United States to foreign embassies).

Paragraph (a)(5) maintains the control on performing a “defense service.”

Paragraph (a)(6) is added for the “release” or transfer of decryption keys,

passwords, and other items identified in the new paragraph (a)(5) of the revised definition of "technical data" in § 120.10. This paragraph makes "release" or transfer of information securing "technical data" an "export." Making the release of decryption keys and other information securing technical data in an inaccessible or unreadable format an export allows the Department to propose that providing someone with encrypted "technical data" would not be an "export," under certain circumstances. Provision of a decryption key or other information securing "technical data" is an "export" regardless of whether the foreign person has already obtained access to the secured "technical data." Paragraph (a)(6) of the definitions of export and reexport in this rule and the BIS companion rule present different formulations for this control and the agencies request input from the public on which language more clearly describes the control. The agencies intend, however, that the act of providing physical access to unsecured "technical data" (subject to the ITAR) will be a controlled event. The mere act of providing access to unsecured technology (subject to the EAR) will not, however, be a controlled event unless it is done with "knowledge" that such provision will cause or permit the transfer of controlled "technology" in clear text or "software" to a foreign national.

Paragraph (a)(7) is added for the release of information to a public network, such as the Internet. This makes more explicit the existing control in (a)(4), which includes the publication of "technical data" to the Internet due to its inherent accessibility by foreign persons. This means that before posting information to the Internet, you should determine whether the information is "technical data." You should review the USML, and if there is doubt about whether the information is "technical data," you may request a commodity jurisdiction determination from the Department. If so, a license or other authorization, as described in § 120.11(b), will generally be required to post such "technical data" to the Internet. Posting "technical data" to the Internet without a Department or other authorization is a violation of the ITAR even absent specific knowledge that a foreign national will read the "technical data."

Paragraph (b)(1) is added to clarify existing ITAR controls to explicitly state that disclosing "technical data" to a foreign person is deemed to be an "export" to all countries in which the

foreign person has held citizenship or holds permanent residency.

8. Revised Definition of Reexport

The Department proposes to revise the definition of "reexport" in ITAR § 120.19 to better align with the EAR's revised definition and describe transfers of items subject to the jurisdiction of the ITAR between two foreign countries. The activities identified are the same as those in paragraphs (a)(1) through (4) of the revised definition of "export," except that the shipment, release or transfer is between two foreign countries or is to a third country national foreign person outside of the United States.

9. Proposed Definition of Release

The Department proposes to add § 120.50, the definition of "release." This term is added to harmonize with the EAR, which has long used the term to cover activities that disclose information to foreign persons. "Release" includes the activities encompassed within the undefined term "disclose." The activities that are captured include allowing a foreign person to inspect a "defense article" in a way that reveals "technical data" to the foreign persons and oral or written exchanges of "technical data" with a foreign person. The adoption of the definition of "release" does not change the scope of activities that constitute an "export" and other controlled transactions under the ITAR.

10. Proposed Definition of Retransfer

The Department proposes to add § 120.51, the definition of "retransfer." "Retransfer" is moved out of the definition of "reexport" in § 120.19 to better harmonize with the EAR, which controls "exports," "reexports" and "transfers (in country)" as discrete events. Under this new definition, a "retransfer" occurs with a change of end use or end user within the same foreign territory. Certain activities may fit within the definition of "reexport" and "retransfer," such as the disclosure of "technical data" to a third country national abroad. Requests for both "reexports" and "retransfers" of "defense articles" will generally be processed through a General Correspondence or an exemption.

11. Proposed Activities That Are Not Exports, Reexports, or Retransfers

The Department proposes to add § 120.52 to describe those "activities that are not exports, reexports, or retransfers" and do not require authorization from the Department. It is not an "export" to launch items into

space, provide "technical data" or software to U.S. persons while in the United States, or move a "defense article" between the states, possessions, and territories of the United States. The Department also proposes to add a new provision excluding from ITAR licensing requirements the transmission and storage of encrypted "technical data" and software.

The Department recognizes that ITAR-controlled "technical data" may be electronically routed through foreign servers unbeknownst to the original sender. This presents a risk of unauthorized access and creates a potential for inadvertent ITAR violations. For example, email containing "technical data" may, without the knowledge of the sender, transit a foreign country's Internet service infrastructure en route to its intended and authorized final destination. Any access to this data by a foreign person would constitute an unauthorized "export" under ITAR § 120.17. Another example is the use of mass data storage (*i.e.*, "cloud storage"). In this case, "technical data" intended to be resident in cloud storage may, without the knowledge of the sender, be physically stored on a server or servers located in a foreign country or multiple countries. Any access to this data, even if unintended by the sender, would constitute an "export" under ITAR § 120.17.

The intent of the proposed ITAR § 120.52(a)(4) is to clarify that when unclassified "technical data" transits through a foreign country's Internet service infrastructure, a license or other approval is not mandated when such "technical data" is encrypted prior to leaving the sender's facilities and remains encrypted until received by the intended recipient or retrieved by the sender, as in the case of remote storage. The encryption must be accomplished in a manner that is certified by the U.S. National Institute for Standards and Technology (NIST) as compliant with the Federal Information Processing Standards Publication 140-2 (FIPS 140-2). Additionally, the Department proposes that the electronic storage abroad of "technical data" that has been similarly encrypted would not require an authorization, so long as it is not stored in a § 126.1 country or in the Russian Federation. This will allow for cloud storage of encrypted data in foreign countries, so long as the "technical data" remains continuously encrypted while outside of the United States.

12. Revised Exemption for the Export of Technical Data for U.S. Persons Abroad

The Department proposes to revise § 125.4(b)(9) to better harmonize controls on the "release" of controlled information to U.S. persons abroad and to update the provisions. The most significant update is that foreign persons authorized to receive "technical data" in the United States will be eligible to receive that same "technical data" abroad, when on temporary assignment on behalf of their employer. The proposed revisions clarify that a person going abroad may use this exemption to "export" "technical data" for their own use abroad. The proposed revisions also clarify that the "technical data" must be secured while abroad to prevent unauthorized "release." It has been long-standing Department practice to hold U.S. persons responsible for the "release" of "technical data" in their possession while abroad. However, given the nature of "technical data" and the proposed exception from licensing for transmission of secured "technical data," the Department has determined it is necessary to implement an affirmative obligation to secure data while abroad.

13. Proposed Scope of License

The Department proposes to add § 123.28 to clarify the scope of a license, in the absence of a proviso, and to state that authorizations are granted based on the information provided by the applicant. This means that while providing false information to the U.S. government as part of the application process for the "export," "reexport," or "retransfer" of a "defense article" is a violation of the ITAR, it also may void the license.

14. Revised Definition of Defense Service

Proposed revisions of the "defense service" definition were published on April 13, 2011, RIN 1400-AC80 (*see* "International Traffic in Arms Regulations: Defense Services," 76 FR 20590) and May 24, 2013 (*see* 78 FR 31444, RIN 1400-AC80). In those rules, the Department explained its determination that the scope of the current definition is overly broad, capturing certain forms of assistance or services that no longer warrant ITAR control.

The Department reviewed comments on that first proposed definition and, when the recommended changes added to the clarity of the regulation, the Department accepted them. For the Department's evaluation of those public comments and recommendations regarding the April 13, 2011, proposed

rule (the first revision), *see* 78 FR 31444, May 24, 2013. The Department's evaluation of the written comments and recommendations in response to the May 24, 2013 proposed rule (the second revision) follows.

Parties commenting on the second revision expressed concern that the definition of "defense service" in paragraph (a)(1) was premised on the use of "other than public domain information." The observation was made that with the intent of removing from the definition of a "defense service" the furnishing of assistance using "public domain" information, but not basing the assistance on the use of "technical data," the Department was continuing to require the licensing of activities akin to those that were based on the use of "public domain" information. The Department has fully revised paragraph (a)(1) to remove the use of the "other than public domain information" or "technical data" from the determination of whether an activity is a "defense service." Furthermore, the Department has added a new provision declaring that the activities described in paragraph (a)(1) are not a "defense service" if performed by a U.S. person or foreign person in the United States who does not have knowledge of U.S.-origin "technical data" directly related to the "defense article" that is the subject of the assistance or training or another "defense article" described in the same USML paragraph prior to performing the service. A note is added to clarify that a person will be deemed to have knowledge of U.S.-origin "technical data" if the person previously participated in the "development" of a "defense article" described in the same USML paragraph, or accessed (physically or electronically) that "technical data." A note is also added to clarify that those U.S. persons abroad who only received U.S.-origin "technical data" as a result of their activities on behalf of a foreign person are not included within the scope of paragraph (a)(1). A third note is added to clarify that DDTC-authorized foreign person employees in the United States who provide "defense services" on behalf of their U.S. employer are considered to be included with the U.S. employer's authorization, and need not be listed on the U.S. employer's technical assistance agreement or receive a separate authorization for those services. The Department also removed the activities of design, development, and engineering from paragraph (a)(1) and moved them to paragraph (a)(2).

Commenting parties recommended revising paragraph (a)(1) to remove the

provision of "technical data" as a "defense service," because there are already licensing requirements for the "export" of "technical data." The Department confirms that it eliminated from the definition of a "defense service" the act of furnishing "technical data" to a foreign person. Such activity still constitutes an "export" and would require an ITAR authorization. New paragraph (a)(1) is concerned with the furnishing of assistance, whereas the "export" of "technical data" alone, without the furnishing of assistance, is not a "defense service." The "export" of "technical data" requires an authorization (Department of State form DSP-5 or DSP-85) or the use of an applicable exemption.

Commenting parties recommended the definition be revised to explicitly state that it applies to the furnishing of assistance by U.S. persons, or by foreign persons in the United States. The Department partially accepted this recommendation. However, the Department notes that ITAR § 120.1(c) provides that only U.S. persons and foreign governmental entities in the United States may be granted a license or other approval pursuant to the ITAR, and that foreign persons may only receive a "reexport" or "retransfer" approval or approval for brokering activities. Therefore, approval for the performance of a defense service in the United States by a foreign person must be obtained by a U.S. person, such as an employer, on behalf of the foreign person. Regarding a related recommendation, the Department also notes that the furnishing of a type of assistance described by the definition of a "defense service" is not an activity within the Department's jurisdiction when it is provided by a foreign person outside the United States to another foreign person outside the United States on a foreign "defense article" using foreign-origin "technical data."

In response to commenting parties, the Department specified that the examples it provided for activities that are not "defense services" are not exhaustive. Rather, they are provided to answer the more frequent questions the Department receives on the matter. The Department removed these examples from paragraph (b) and included them as a note to paragraph (a).

A commenting party recommended that paragraphs (a)(5) and (a)(6), regarding the furnishing of assistance in the integration of a spacecraft to a launch vehicle and in the launch failure analysis of a spacecraft or launch vehicle, respectively, be removed, and that those activities be described in the USML categories covering spacecraft

and launch vehicles, on the basis that a general definition should not have such program-specific clauses. As discussed in the May 13, 2014 interim final rule revising USML Category XV (79 FR 27180), the Department accepted this recommendation and revised paragraph (f) of USML Category XV and paragraph (i) of USML Category IV accordingly. The revision includes the recommendation of commenting parties to specifically provide that the service must be provided to a foreign person in order for it to be a licensable activity.

Commenting parties recommended the Department define the term "tactical employment," so as to clarify what services would be captured by paragraph (a)(3). The Department determined that employment of a "defense article" should remain a controlled event, due to the nature of items now controlled in the revised USML categories. After ECR, those items that remain "defense articles" are the most sensitive and militarily critical equipment that have a significant national security or intelligence application. Allowing training and other services to foreign nationals in the employment of these "defense articles" without a license would not be appropriate. Therefore, the Department removed the word "tactical" and converted the existing exemption for basic operation of a "defense article," authorized by the U.S. government for "export" to the same recipient, into an exclusion from paragraph (a)(3).

A commenting party recommended the Department address the instance of the integration or installation of a "defense article" into an item, much as it addressed the instance of the integration or installation of an item into a "defense article." Previously, the Department indicated this would be the subject of a separate rule, and addressed the "export" of such items in a proposed rule (*see* 76 FR 13928), but upon review the Department accepted this recommendation, and revised paragraph (a)(2), the note to paragraph (a)(2), and the note to paragraph (a) accordingly. In addition, the Department has changed certain terminology used in the paragraph: instead of referring to the "transfer" of "technical data," the paragraph is premised on the "use" of "technical data." This change is consistent with removing from the definition of a "defense service" the furnishing of "technical data" to a foreign person when there is not also the furnishing of assistance related to that "technical data."

A commenting party requested clarification of the rationale behind

selectively excepting from the "defense services" definition the furnishing of services using "public domain" information. The Department did so in paragraph (a)(1), and now excludes those services performed by U.S. persons who have not previously had access to any U.S. origin "technical data" on the "defense article" being serviced. In contrast, the Department did not do so in paragraphs (a)(2) and (a)(3) and former paragraphs (a)(5) and (a)(6). In the case of paragraph (a)(2), the rationale for not doing so is that the activities involved in the development of a "defense article," or in integrating a "defense article" with another item, inherently involve the advancement of the military capacity of another country and therefore constitute activities over which the U.S. government has significant national security and foreign policy concerns. To the extent that an activity listed in paragraph (a)(1), such as modification or testing, is done in the "development" of a "defense article," such activities constitute "development" and are within the scope of paragraph (a)(2). With regard to paragraph (a)(3), the furnishing of assistance (including training) in the employment of a "defense article" is a type of activity that the Department believes warrants control as a "defense service," due to the inherently military nature of providing training and other services in the employment of a "defense article" (changes to paragraph (a)(3) are described above). The services described in former paragraphs (a)(5) and (a)(6) (and now in USML Categories IV(i) and XV(f)) are pursuant to Public Law 105-261.

A commenting party recommended limiting paragraph (a)(2) to the integration of ECCN 9A515 and 600 series items into defense articles, saying that the regulations should focus on items subject to the EAR with a military or space focus. The Department's focus with this provision is in fact the "defense article." Items that are to be integrated with a "defense article," which may not themselves be defense articles, may be beyond the authority of the Department to regulate. The Department did not accept this recommendation.

A commenting party recommended limiting the definition of integration to changes in the function of the "defense article," and to exclude modifications in fit. For the purposes of illustration, this commenting party used one of the examples provided by the Department in the note to paragraph (a)(2): The manufacturer of the military vehicle will need to know the dimensions and electrical requirements of the dashboard

radio when designing the vehicle. In this instance, paragraph (a)(2) would not apply, as this example addresses the manufacture of a "defense article," which is covered by paragraph (a)(1). If the radio to be installed in this vehicle is subject to the EAR, the provision to the manufacturer of information regarding the radio is not within the Department's licensing jurisdiction. In an instance of a service entailing the integration of an item with a "defense article," where there would be modification to any of the items, the Department believes such assistance would inherently require the use of "technical data." Therefore, this exclusion would be unacceptably broad. However, the Department has accepted the recommendation to clarify the definition and exclude changes to fit to any of the items involved in the integration activity, provided that such services do not entail the use of "technical data" directly related to the "defense article." Upon review, changes to fit are not an aspect of integration, which is the "engineering analysis needed to unite a 'defense article' and one or more items," and therefore are not captured in paragraph (a)(2). The modifications of the "defense article" to accommodate the fit of the item to be integrated, which are within the activity covered by installation, are only those modifications to the "defense article" that allow the item to be placed in its predetermined location. Any modifications to the design of a "defense article" are beyond the scope of installation. Additionally, while minor modifications may be made to a "defense article" without the activity being controlled under (a)(2) as an integration activity, all modifications of defense articles, regardless of sophistication, are activities controlled under (a)(1) if performed by someone with prior knowledge of U.S.-origin "technical data." "Fit" is defined in ITAR § 120.41: "The fit of a commodity is defined by its ability to physically interface or connect with or become an integral part of another commodity" (*see*, Note 4 to paragraph (b)(3)).

Commenting parties recommended revising paragraph (a)(2) to provide that such assistance described therein would be a "defense service" only if U.S.-origin "technical data" is exported. The law and regulations do not mandate this limitation. Section 38 of the Arms Export Control Act provides that the President is authorized to control the "export" of defense articles and defense services. The ITAR, in defining "defense article," "technical data," and "export," does not provide the qualifier "U.S.-

origin" (see ITAR §§ 120.6, 120.10, and 120.17, respectively). In the instance described by the commenting party, of the integration of a commercial item into a foreign-origin "defense article," the Department retains jurisdiction when the service is provided by a U.S. person.

A commenting party recommended revising paragraph (a)(2) so that the paragraph (a)(1) exception of the furnishing of assistance using "public domain" information is not nullified by paragraph (a)(2), as most of the activities described in paragraph (a)(1) involve integration as defined in the note to paragraph (a)(2). The Department believes each of the activities described in paragraphs (a)(1) and (a)(2) are sufficiently well defined to distinguish them one from the other. Therefore, the Department does not agree that paragraph (a)(2) nullifies the intention of paragraph (a)(1), and does not accept this recommendation.

A commenting party requested clarification that providing an item subject to the EAR for the purposes of integration into a "defense article" is not a "defense service." The provision of the item in this instance, unaccompanied by assistance in the integration of the item into a "defense article," is not within the scope of "the furnishing of assistance," and therefore is not a defense service.

Commenting parties recommended clarification on whether the servicing of an item subject to the EAR that has been integrated with a "defense article" would be a "defense service." The Department notes that such activity is not a "defense service," provides it as an example of what is not a "defense service" in the note to paragraph (a), and also notes that it would be incumbent on the applicant to ensure that in providing this service, "technical data" directly related to the "defense article" is not used.

Commenting parties expressed concern over the potential negative effect of paragraph (a)(2) and the definition in general on university-based educational activities and scientific communication, and recommended clarification of the relationship between the definition of "defense services" and the exemption for the "export" of "technical data" at ITAR § 125.4(b)(10). Disclosures of "technical data" to foreign persons who are bona-fide and full time regular employees of universities continue to be exports for which ITAR § 125.4(b)(10) is one licensing exemption. The Department believes that, in most cases, the normal duties of a university employee do not encompass the

furnishing of assistance to a foreign person, in the activities described in paragraph (a). Therefore, in the context of employment with the university, the Department does not perceive that the foreign person's use of the "technical data" would be described by ITAR § 120.9(a)(2), or any part of paragraph (a).

In response to the recommendation of one commenting party, the Department added a note clarifying that the installation of an item into a "defense article" is not a "defense service," provided no "technical data" is used in the rendering of the service.

A commenting party recommended clarification of the licensing process for the "export" of an EAR 600 series item that is to be integrated into a "defense article." The Department of Commerce has "export" authority over the 600 series item, and the exporter must obtain a license from the Department of Commerce, if necessary. The exporter must also obtain an approval from the Department of State to provide any "defense service," including integration assistance pursuant to paragraph (a)(2).

A commenting party recommended removing "testing" as a type of "defense service," stating it was not included in the definition of "organizational-level maintenance." In including testing as part of the former definition but not of the latter, the Department does not perceive an inconsistency or conflict. To the extent that certain testing is within the definition of organization-level maintenance, that testing is explicitly excluded, as organizational-level maintenance is not covered under the definition of a "defense service." However, all other testing remains a "defense service." The Department intends for the furnishing of assistance to a foreign person, whether in the United States or abroad, in the testing of defense articles to be an activity requiring Department approval under the conditions of paragraph (a)(1). The Department did not accept this recommendation.

Commenting parties provided recommendations for revising the definitions of "public domain" information and "technical data." Those definitions are proposed in this rule as well. To the extent that evaluation of the proposed changes to "defense services" hinges on these terms, the Department invites commenting parties to submit analyses of the impact of these revised definitions on the revised "defense service" definition in this proposed rule.

Commenting parties recommended clarification of the regulation regarding the furnishing of assistance and training

in organizational-level (basic-level) maintenance. The Department harmonized paragraph (a)(1) and the example regarding organizational-level maintenance by revising the Note to Paragraph (a), which sets forth activities that are not "defense services," so that it specifically provides that "the furnishing of assistance (including training) in organizational-level (basic-level) maintenance of a defense article" is an example of an activity that is not a defense service.

In response to commenting parties, the Department clarifies that the example of employment by a foreign person of a natural U.S. person as not constituting a "defense service" is meant to address, among other scenarios, the instance where such a person is employed by a foreign defense manufacturer, but whose employment in fact does not entail the furnishing of assistance as described in ITAR § 120.9(a). By "natural person," the Department means a human being, as may be inferred from the definition of "person" provided in ITAR § 120.14.

In response to the recommendation of a commenting party, the Department confirms that, as stated in a Department of Commerce notice, "Technology subject to the EAR that is used with technical data subject to the ITAR that will be used under the terms of a Technical Assistance Agreement (TAA) or Manufacturing License Agreement (MLA) and that would otherwise require a license from [the Department of Commerce] may all be exported under the TAA or MLA" (see 78 FR 22660). In DDTC publication *Guidelines for Preparing Electronic Agreements (Revision 4.2)*, Section 20.1.d., the following conditions are stipulated: The technology subject to the EAR will be used with "technical data" subject to the ITAR and described in the agreement, and the technology subject to the EAR will be used under the terms of a TAA or MLA (see <http://www.pmddtc.state.gov/licensing/agreement.html>).

Request for Comments

The Department invites public comment on any of the proposed definitions set forth in this rulemaking. With respect to the revisions to ITAR § 120.17, the Department recognizes the increasingly complex nature of telecommunications infrastructure and the manner in which data is transmitted, stored, and accessed, and accordingly seeks public comment with special emphasis on: (1) How adequately the proposed regulations address the technical aspects of data transmission and storage; (2) whether

the proposed regulations mitigate unintended or unauthorized access to transmitted or stored data; and (3) whether the proposed regulations impose an undue financial or compliance burden on the public.

The public is also asked to comment on the effective date of the final rule. Export Control Reform rules that revised categories of the USML and created new 600 series ECCN have had a six-month delayed effective date to allow for exporters to update the classification of their items. In general, rules effecting export controls have been effective on the date of publication, due to the impact on national security and foreign policy. As this proposed rule and the companion proposed rule from the Bureau of Industry and Security revise definitions within the ITAR and the EAR and do not make any changes to the USML or CCL, the Department proposes (should the proposed rule be adopted) a 30-day delayed effective date to allow exporters to ensure continued compliance.

Regulatory Analysis and Notices

Administrative Procedure Act

The Department of State is of the opinion that controlling the import and export of defense articles and services is a foreign affairs function of the U.S. government and that rules implementing this function are exempt from sections 553 (rulemaking) and 554 (adjudications) of the Administrative Procedure Act (APA). Although the Department is of the opinion that this proposed rule is exempt from the rulemaking provisions of the APA, the Department is publishing this rule with a 60-day provision for public comment and without prejudice to its determination that controlling the import and export of defense services is a foreign affairs function.

Regulatory Flexibility Act

Since the Department is of the opinion that this proposed rule is exempt from the rulemaking provisions of 5 U.S.C. 553, there is no requirement for an analysis under the Regulatory Flexibility Act.

Unfunded Mandates Reform Act of 1995

This proposed amendment does not involve a mandate that will result in the expenditure by State, local, and tribal governments, in the aggregate, or by the private sector, of \$100 million or more in any year and it will not significantly or uniquely affect small governments. Therefore, no actions were deemed necessary under the provisions of the

Unfunded Mandates Reform Act of 1995.

Small Business Regulatory Enforcement Fairness Act of 1996

For purposes of the Small Business Regulatory Enforcement Fairness Act of 1996 (the "Act"), a major rule is a rule that the Administrator of the OMB Office of Information and Regulatory Affairs finds has resulted or is likely to result in: (1) An annual effect on the economy of \$100,000,000 or more; (2) a major increase in costs or prices for consumers, individual industries, federal, state, or local government agencies, or geographic regions; or (3) significant adverse effects on competition, employment, investment, productivity, innovation, or on the ability of United States-based enterprises to compete with foreign-based enterprises in domestic and foreign markets.

The Department does not believe this rulemaking will have an annual effect on the economy of \$100,000,000 or more, nor will it result in a major increase in costs or prices for consumers, individual industries, federal, state, or local government agencies, or geographic regions, or have significant adverse effects on competition, employment, investment, productivity, innovation, or on the ability of United States-based enterprises to compete with foreign-based enterprises in domestic and foreign markets. The proposed means of solving the issue of data protection are both familiar to and extensively used by the affected public in protecting sensitive information.

Executive Orders 12372 and 13132

This proposed amendment will not have substantial direct effects on the States, on the relationship between the national government and the States, or on the distribution of power and responsibilities among the various levels of government. Therefore, in accordance with Executive Order 13132, it is determined that this proposed amendment does not have sufficient federalism implications to require consultations or warrant the preparation of a federalism summary impact statement. The regulations implementing Executive Order 12372 regarding intergovernmental consultation on Federal programs and activities do not apply to this proposed amendment.

Executive Orders 12866 and 13563

Executive Orders 12866 and 13563 direct agencies to assess costs and benefits of available regulatory

alternatives and, if regulation is necessary, to select regulatory approaches that maximize net benefits (including potential economic, environmental, public health and safety effects, distributed impacts, and equity). The executive orders stress the importance of quantifying both costs and benefits, of reducing costs, of harmonizing rules, and of promoting flexibility. This proposed rule has been designated a "significant regulatory action," although not economically significant, under section 3(f) of Executive Order 12866. Accordingly, the proposed rule has been reviewed by the Office of Management and Budget (OMB).

Executive Order 12988

The Department of State has reviewed the proposed amendment in light of sections 3(a) and 3(b)(2) of Executive Order 12988 to eliminate ambiguity, minimize litigation, establish clear legal standards, and reduce burden.

Executive Order 13175

The Department of State has determined that this rulemaking will not have tribal implications, will not impose substantial direct compliance costs on Indian tribal governments, and will not preempt tribal law. Accordingly, Executive Order 13175 does not apply to this rulemaking.

Paperwork Reduction Act

This rule does not impose any new reporting or recordkeeping requirements subject to the Paperwork Reduction Act, 44 U.S.C. Chapter 35; however, the Department of State seeks public comment on any unforeseen potential for increased burden.

List of Subjects

22 CFR 120 and 125

Arms and munitions, Classified information, Exports.

22 CFR 123

Arms and munitions, Exports, Reporting and recordkeeping requirements.

22 CFR Part 127

Arms and munitions, Exports, Crime, Law, Penalties, Seizures and forfeitures.

Accordingly, for the reasons set forth above, title 22, chapter I, subchapter M, parts 120, 123, 125, and 127 are proposed to be amended as follows:

PART 120—PURPOSE AND DEFINITIONS

■ 1. The authority citation for part 120 continues to read as follows:

Authority: Secs. 2, 38, and 71, Pub. L. 90-629, 90 Stat. 744 (22 U.S.C. 2752, 2778, 2797); 22 U.S.C. 2794; 22 U.S.C. 2651a; Pub. L. 105-261, 112 Stat. 1920; Pub. L. 111-266; Section 1261, Pub. L. 112-239; E.O. 13637, 78 FR 16129.

■ 2. Section 120.6 is amended by designating the current text as paragraph (a), revising the first sentence of newly designated paragraph (a), and adding paragraph (b) to read as follows:

§ 120.6 Defense article.

(a) *Defense article* means any item, software, or technical data designated in § 121.1 of this subchapter. * * *

(b) The following are not defense articles and thus not subject to the ITAR:

- (1) [Reserved]
- (2) [Reserved]
- (3) Information and software that:
 - (i) Are in the public domain, as described in § 120.11;
 - (ii) Arise during, or result from, fundamental research, as described in § 120.46;
 - (iii) Concern general scientific, mathematical, or engineering principles commonly taught in schools, and released by instruction in a catalog course or associated teaching laboratory of an academic institution; or
 - (iv) Appear in patents or open (published) patent applications available from or at any patent office, unless covered by an invention secrecy order.

Note to paragraph (b): Information that is not within the scope of the definition of technical data (see § 120.10) and not directly related to a defense article, or otherwise described on the USML, is not subject to the ITAR.

■ 3. Section 120.9 is revised to read as follows:

§ 120.9 Defense service.

(a) *Defense service* means:

- (1) The furnishing of assistance (including training) to a foreign person (see § 120.16), whether in the United States or abroad, in the production, assembly, testing, intermediate- or depot-level maintenance (see § 120.38), modification, demilitarization, destruction, or processing of a defense article (see § 120.6), by a U.S. person or foreign person in the United States, who has knowledge of U.S.-origin technical data directly related to the defense article that is the subject of the assistance, prior to performing the service;

Note 1 to paragraph (a)(1): "Knowledge of U.S.-origin technical data" for purposes of paragraph (a)(1) can be established based on all the facts and circumstances. However, a person is deemed to have "knowledge of

U.S.-origin technical data" directly related to a defense article if the person participated in the development of a defense article described in the same USML paragraph or accessed (physically or electronically) technical data directly related to the defense article that is the subject of the assistance, prior to performing the service.

Note 2 to paragraph (a)(1): U.S. persons abroad who only receive U.S.-origin technical data as a result of their activities on behalf of a foreign person are not included within paragraph (a)(1).

Note 3 to paragraph (a)(1): Foreign person employees in the United States providing defense services as part of Directorate of Defense Trade Controls-authorized employment need not be listed on the U.S. employer's technical assistance agreement or receive separate authorization to perform defense services on behalf of their authorized U.S. employer.

(2) The furnishing of assistance (including training) to a foreign person (see § 120.16), whether in the United States or abroad, in the development of a defense article, or the integration of a defense article with any other item regardless of whether that item is subject to the ITAR or technical data is used;

Note to paragraph (a)(2): "Integration" means any engineering analysis (see § 125.4(c)(5) of this subchapter) needed to unite a defense article and one or more items. Integration includes the introduction of software to enable operation of a defense article, and the determination during the design process of where an item will be installed (e.g., integration of a civil engine into a destroyer that requires changes or modifications to the destroyer in order for the civil engine to operate properly; not plug and play). Integration is distinct from "installation." Installation means the act of putting an item in its predetermined place without the use of technical data or any modifications to the defense article involved, other than to accommodate the fit of the item with the defense article (e.g., installing a dashboard radio into a military vehicle where no modifications (other than to accommodate the fit of the item) are made to the vehicle, and there is no use of technical data.). The "fit" of an item is defined by its ability to physically interface or connect with or become an integral part of another item. (see § 120.41).

(3) The furnishing of assistance (including training) to a foreign person (see § 120.16), regardless of whether technical data is used, whether in the United States or abroad, in the employment of a defense article, other than basic operation of a defense article authorized by the U.S. government for export to the same recipient;

(4) Participating in or directing combat operations for a foreign person (see § 120.16), except as a member of the regular military forces of a foreign

nation by a U.S. person who has been drafted into such forces; or

(5) The furnishing of assistance (including training) to the government of a country listed in § 126.1 of this subchapter in the development, production, operation, installation, maintenance, repair, overhaul or refurbishing of a defense article or a part component, accessory or attachments specially designed for a defense article.

Note to paragraph (a): The following are examples of activities that are not defense services:

1. The furnishing of assistance (including training) in organizational-level (basic-level) maintenance (see § 120.38) of a defense article;
2. Performance of services by a U.S. person in the employment of a foreign person, except as provided in this paragraph;
3. Servicing of an item subject to the EAR (see § 120.42) that has been integrated or installed into a defense article, or the servicing of an item subject to the EAR into which a defense article has been installed or integrated, without the use of technical data, except as described in paragraph (a)(5) of this section;
4. The installation of any item into a defense article, or the installation of a defense article into any item;
5. Providing law enforcement, physical security, or personal protective services (including training and advice) to or for a foreign person (if such services necessitate the export of a defense article a license or other approval is required for the export of the defense article, and such services that entail the employment or training in the employment of a defense article are addressed in paragraph (a)(3) of this section);
6. The furnishing of assistance by a foreign person not in the United States;
7. The furnishing of medical, logistical (other than maintenance), translation, financial, legal, scheduling, or administrative services;
8. The furnishing of assistance by a foreign government to a foreign person in the United States, pursuant to an arrangement with the Department of Defense; and
9. The instruction in general scientific, mathematical, or engineering principles commonly taught in schools, colleges, and universities.

(b) [Reserved]

■ 4. Section 120.10 is revised to read as follows:

§ 120.10 Technical data.

(a) *Technical data* means, except as set forth in paragraph (b) of this section:

- (1) Information required for the development (see § 120.47) (including design, modification, and integration design), production (see § 120.48) (including manufacture, assembly, and integration), operation, installation, maintenance, repair, overhaul, or refurbishing of a defense article. Technical data may be in any tangible or intangible form, such as written or

oral communications, blueprints, drawings, photographs, plans, diagrams, models, formulae, tables, engineering designs and specifications, computer-aided design files, manuals or documentation, electronic media or information gleaned through visual inspection;

Note to paragraph (a)(1): The modification of an existing item creates a new item and technical data for the modification is technical data for the development of the new item.

(2) Information enumerated on the USML (*i.e.*, not controlled pursuant to a catch-all USML paragraph);

(3) Classified information for the development, production, operation, installation, maintenance, repair, overhaul, or refurbishing of a defense article or a 600 series item subject to the EAR;

(4) Information covered by an invention secrecy order; or

(5) Information, such as decryption keys, network access codes, or passwords, that would allow access to other technical data in clear text or software (*see* § 127.1(b)(4) of this subchapter).

(b) *Technical data does not include:*

(1) Non-proprietary general system descriptions;

(2) Information on basic function or purpose of an item; or

(3) Telemetry data as defined in note 3 to USML Category XV(f) (*see* § 121.1 of this subchapter).

■ 5. Section 120.11 is revised to read as follows:

§ 120.11 Public domain.

(a) Except as set forth in paragraph (b) of this section, unclassified information and software are in the public domain, and are thus not technical data or software subject to the ITAR, when they have been made available to the public without restrictions upon their further dissemination such as through any of the following:

(1) Subscriptions available without restriction to any individual who desires to obtain or purchase the published information;

(2) Libraries or other public collections that are open and available to the public, and from which the public can obtain tangible or intangible documents;

(3) Unlimited distribution at a conference, meeting, seminar, trade show, or exhibition, generally accessible to the interested public;

(4) Public dissemination (*i.e.*, unlimited distribution) in any form (*e.g.*, not necessarily in published form), including posting on the Internet on sites available to the public; or

(5) Submission of a written composition, manuscript or presentation to domestic or foreign co-authors, editors, or reviewers of journals, magazines, newspapers or trade publications, or to organizers of open conferences or other open gatherings, with the intention that the compositions, manuscripts, or publications will be made publicly available if accepted for publication or presentation.

(b) Technical data or software, whether or not developed with government funding, is not in the public domain if it has been made available to the public without authorization from:

(1) The Directorate of Defense Trade Controls;

(2) The Department of Defense's Office of Security Review;

(3) The relevant U.S. government contracting entity with authority to allow the technical data or software to be made available to the public; or

(4) Another U.S. government official with authority to allow the technical data or software to be made available to the public.

Note 1 to § 120.11: Section 127.1(a)(6) of this subchapter prohibits, without written authorization from the Directorate of Defense Trade Controls, U.S. and foreign persons from exporting, reexporting, retransferring, or otherwise making available to the public technical data or software if such person has knowledge that the technical data or software was made publicly available without an authorization described in paragraph (b) of this section.

Note 2 to § 120.11: An export, reexport, or retransfer of technical data or software that was made publicly available by another person without authorization is not a violation of this subchapter, except as described in § 127.1(a)(6) of this subchapter.

■ 6. Section 120.17 is revised to read as follows:

§ 120.17 Export.

(a) Except as set forth in § 120.52, § 126.16, or § 126.17 of this subchapter, *export* means:

(1) An actual shipment or transmission out of the United States, including the sending or taking of a defense article outside of the United States in any manner;

(2) Releasing or otherwise transferring technical data or software (source code or object code) to a foreign person in the United States (a "deemed export");

(3) Transferring by a person in the United States of registration, control, or ownership of any aircraft, vessel, or satellite subject to the ITAR to a foreign person;

(4) Releasing or otherwise transferring a defense article to an embassy or to any

agency or subdivision of a foreign government, such as a diplomatic mission, in the United States;

(5) Performing a defense service on behalf of, or for the benefit of, a foreign person, whether in the United States or abroad;

(6) Releasing or otherwise transferring information, such as decryption keys, network access codes, passwords, or software, or providing physical access, that would allow access to other technical data in clear text or software to a foreign person regardless of whether such data has been or will be transferred; or

(7) Making technical data available via a publicly available network (*e.g.*, the Internet).

(b) Any release in the United States of technical data or software to a foreign person is a deemed export to all countries in which the foreign person has held citizenship or holds permanent residency.

■ 7. Section 120.19 is revised to read as follows:

§ 120.19 Reexport.

(a) Except as set forth in § 120.52, *reexport* means:

(1) An actual shipment or transmission of a defense article from one foreign country to another foreign country, including the sending or taking of a defense article to or from such countries in any manner;

(2) Releasing or otherwise transferring technical data or software to a foreign person of a country other than the foreign country where the release or transfer takes place (a "deemed reexport");

(3) Transferring by a person outside of the United States of registration, control, or ownership of any aircraft, vessel, or satellite subject to the ITAR to a foreign person outside the United States; or

(4) Releasing or otherwise transferring outside of the United States information, such as decryption keys, network access codes, password, or software, or providing physical access, that would allow access to other technical data in clear text or software to a foreign person regardless of whether such data has been or will be transferred.

(b) [Reserved]

§ 120.41 [Amended]

■ 8. Section 120.41 is amended by reserving Note 1 to paragraph (b)(3) and Note 2 to paragraph (b)(3).

■ 9. Section 120.46 is added to read as follows:

§ 120.46 Required.

(a) As applied to technical data, the term *required* refers to only that portion

of technical data that is peculiarly responsible for achieving or exceeding the controlled performance levels, characteristics, or functions. Such required technical data may be shared by different products.

Note 1 to paragraph (a): The references to "characteristics" and "functions" are not limited to entries on the USML that use specific technical parameters to describe the scope of what is controlled. The "characteristics" and "functions" of an item listed are, absent a specific regulatory definition, a standard dictionary's definition of the item. For example, USML Category VIII(a)(1) controls aircraft that are "bombers." No performance level is identified in the entry, but the characteristic of the aircraft that is controlled is that it is a bomber. Thus, any technical data, regardless of significance, peculiar to making an aircraft a bomber as opposed to, for example, an aircraft controlled under ECCN 9A610.a or ECCN 9A991.a, would be technical data required for a bomber and thus controlled under USML Category VIII(i).

Note 2 to paragraph (a): The ITAR and the EAR often divide within each set of regulations or between each set of regulations:

1. Controls on parts, components, accessories, attachments, and software; and
2. Controls on the end items, systems, equipment, or other items into which those parts, components, accessories, attachments, and software are to be installed or incorporated.

With the exception of technical data specifically enumerated on the USML, the jurisdictional status of unclassified technical data is the same as the jurisdictional status of the defense article or item subject to the EAR to which it is directly related. Thus, if technology is directly related to the production of an ECCN 9A610.x aircraft component that is to be integrated or installed in a USML Category VIII(a) aircraft, the technology is controlled under ECCN 9E610, not USML Category VIII(i).

Note 3 to paragraph (a): Technical data is "peculiarly responsible for achieving or exceeding the controlled performance levels, characteristics, or functions" if it is used in or for use in the development (including design, modification, and integration design), production (including manufacture, assembly, and integration), operation, installation, maintenance, repair, overhaul, or refurbishing of a defense article unless:

1. The Department of State has determined otherwise in a commodity jurisdiction determination;
2. [Reserved];
3. It is identical to information used in or with a commodity or software that:
 - i. Is or was in production (*i.e.*, not in development); and
 - ii. Is not a defense article;
4. It was or is being developed with knowledge that it is for or would be for use in or with both defense articles and commodities not on the U.S. Munitions List; or

5. It was or is being developed for use in or with general purpose commodities or software (*i.e.*, with no knowledge that it would be for use in or with a particular commodity).

(b) [Reserved]

■ 10. Section 120.47 is added to read as follows:

§ 120.47 Development.

Development is related to all stages prior to serial production, such as: design, design research, design analyses, design concepts, assembly and testing of prototypes, pilot production schemes, design data, process of transforming design data into a product, configuration design, integration design, and layouts. Development includes modification of the design of an existing item.

■ 11. Section 120.48 is added to read as follows:

§ 120.48 Production.

Production means all production stages, such as product engineering, manufacture, integration, assembly (mounting), inspection, testing, and quality assurance. This includes "serial production" where commodities have passed production readiness testing (*i.e.*, an approved, standardized design ready for large scale production) and have been or are being produced on an assembly line for multiple commodities using the approved, standardized design.

■ 12. Section 120.49 is added to read as follows:

§ 120.49 Technical data that arises during, or results from, fundamental research.

(a) *Technical Data arising during, or resulting from, fundamental research.* Unclassified information that arises during, or results from, fundamental research and is intended to be published is not technical data when the research is:

- (1) Conducted in the United States at an accredited institution of higher learning located; or
- (2) Funded, in whole or in part, by the U.S. government.

Note 1 to paragraph (a): The inputs used to conduct fundamental research, such as information, equipment, or software, are not "technical data that arises during or results from fundamental research" except to the extent that such inputs are technical data that arose during or resulted from earlier fundamental research.

Note 2 to paragraph (a): There are instances in the conduct of research, whether fundamental, basic, or applied, where a researcher, institution, or company may decide to restrict or protect the release or publication of technical data contained in research results. Once a decision is made to

maintain such technical data as restricted or proprietary, the technical data becomes subject to the ITAR.

(b) *Prepublication review.* Technical data that arises during, or results from, fundamental research is intended to be published to the extent that the researchers are free to publish the technical data contained in the research without any restriction or delay, including U.S. government-imposed access and dissemination controls or research sponsor proprietary information review.

Note 1 to paragraph (b): Although technical data arising during or resulting from fundamental research is not considered "intended to be published" if researchers accept restrictions on its publication, such technical data will nonetheless qualify as technical data arising during or resulting from fundamental research once all such restrictions have expired or have been removed.

Note 2 to paragraph (b): Research that is voluntarily subjected to U.S. government prepublication review is considered intended to be published for all releases consistent with any resulting controls.

Note 3 to paragraph (b): Technical data resulting from U.S. government funded research which is subject to government-imposed access and dissemination or other specific national security controls qualifies as technical data resulting from fundamental research, provided that all government-imposed national security controls have been satisfied.

(c) *Fundamental research definition.* Fundamental research means basic or applied research in science and engineering, the results of which ordinarily are published and shared broadly within the scientific community. This is distinguished from proprietary research and from industrial development, design, production, and product utilization, the results of which ordinarily are restricted for proprietary or national security reasons.

(1) *Basic research* means experimental or theoretical work undertaken principally to acquire new knowledge of the fundamental principles of phenomena or observable facts, not primarily directed towards a specific practical aim or objective.

(2) *Applied research* means the effort that:

(i) Normally follows basic research, but may not be severable from the related basic research;

(ii) Attempts to determine and exploit the potential of scientific discoveries or improvements in technology, materials, processes, methods, devices, or techniques; and

(iii) Attempts to advance the state of the art.

■ 13. Section 120.50 is added to read as follows:

§ 120.50 Release.

(a) Except as set forth in § 120.52, technical data and software are released through:

(1) Visual or other inspection by foreign persons of a defense article that reveals technical data or software to a foreign person; or

(2) Oral or written exchanges with foreign persons of technical data in the United States or abroad.

(b) [Reserved]

■ 14. Section 120.51 is added to read as follows:

§ 120.51 Retransfer.

Except as set forth in § 120.52 of this subchapter, a *retransfer* is a change in end use or end user of a defense article within the same foreign country.

■ 15. Section 120.52 is added to read as follows:

§ 120.52 Activities that are not exports, reexports, or retransfers.

(a) The following activities are not exports, reexports, or retransfers:

(1) Launching a spacecraft, launch vehicle, payload, or other item into space;

(2) While in the United States, releasing technical data or software to a U.S. person;

(3) Shipping, moving, or transferring defense articles between or among the United States, the District of Columbia, the Commonwealth of Puerto Rico, the Commonwealth of the Northern Mariana Islands or any territory, dependency, or possession of the United States as listed in Schedule C, Classification Codes and Descriptions for U.S. Export Statistics, issued by the Bureau of the Census; and

(4) Sending, taking, or storing technical data or software that is:

(i) Unclassified;

(ii) Secured using end-to-end encryption;

(iii) Secured using cryptographic modules (hardware or software) compliant with the Federal Information Processing Standards Publication 140-2 (FIPS 140-2) or its successors, supplemented by software implementation, cryptographic key management and other procedures and controls that are in accordance with guidance provided in current U.S. National Institute for Standards and Technology publications; and

(iv) Not stored in a country proscribed in § 126.1 of this subchapter or the Russian Federation.

(b) For purposes of this section, end-to-end encryption means the provision of uninterrupted cryptographic

protection of data between an originator and an intended recipient, including between an individual and himself or herself. It involves encrypting data by the originating party and keeping that data encrypted except by the intended recipient, where the means to access the data in unencrypted form is not given to any third party, including to any Internet service provider, application service provider or cloud service provider.

(c) The ability to access technical data or software in encrypted form that satisfies the criteria set forth in paragraph (a)(4) of this section does not constitute the release or export of such technical data or software.

Note to § 120.52: See § 127.1 of this subchapter for prohibitions on the release or transfer of technical data or software, in any form, to any person with knowledge that a violation will occur.

PART 123—LICENSES FOR THE EXPORT AND TEMPORARY IMPORT OF DEFENSE ARTICLES

■ 16. The authority citation for part 123 continues to read as follows:

Authority: Secs. 2, 38, and 71, 90 Stat. 744 (22 U.S.C. 2752, 2778, 2797); 22 U.S.C. 2753; 22 U.S.C. 2651a; 22 U.S.C. 2776; Pub. L. 105-261, 112 Stat. 1920; Sec. 1205(a), Pub. L. 107-228; Section 1261, Pub. L. 112-239; E.O. 13637, 78 FR 16129.

■ 17. Section 123.28 is added to read as follows:

§ 123.28 Scope of a license.

Unless limited by a condition set out in a license, the export, reexport, retransfer, or temporary import authorized by a license is for the item(s), end-use(s), and parties described in the license application and any letters of explanation. DDTC grants licenses in reliance on representations the applicant made in or submitted in connection with the license application, letters of explanation, and other documents submitted.

PART 124—AGREEMENTS, OFFSHORE PROCUREMENT, AND OTHER DEFENSE SERVICES

■ 18. The authority citation for part 124 continues to read as follows:

Authority: Secs. 2, 38, and 71, 90 Stat. 744 (22 U.S.C. 2752, 2778, 2797); 22 U.S.C. 2651a; 22 U.S.C. 2776; Section 1514, Pub. L. 105-261; Pub. L. 111-266; Section 1261, Pub. L. 112-239; E.O. 13637, 78 FR 16129.

■ 19. Section 124.1 is amended by adding paragraph (e) to read as follows:

§ 124.1 Manufacturing license agreements and technical assistance agreements.

* * * * *

(e) Unless limited by a condition set out in an agreement, the export, reexport, retransfer, or temporary import authorized by a license is for the item(s), end-use(s), and parties described in the agreement, license, and any letters of explanation. DDTC approves agreements and grants licenses in reliance on representations the applicant made in or submitted in connection with the agreement, letters of explanation, and other documents submitted.

PART 125—LICENSES FOR THE EXPORT OF TECHNICAL DATA AND CLASSIFIED DEFENSE ARTICLES

■ 20. The authority citation for part 125 continues to read as follows:

Authority: Secs. 2 and 38, 90 Stat. 744 (22 U.S.C. 2752, 2778); 22 U.S.C. 2651a; E.O. 13637, 78 FR 16129.

■ 21. Section 125.4 is amended by revising paragraph (b)(9) to read as follows:

§ 125.4 Exemptions of general applicability.

* * * * *

(b) * * *

(9) Technical data, including classified information, regardless of media or format, exported by or to a U.S. person or a foreign person employee of a U.S. person, travelling or on temporary assignment abroad subject to the following restrictions:

(i) Foreign persons may only export or receive such technical data as they are authorized to receive through a separate license or other approval.

(ii) The technical data exported under this authorization is to be possessed or used solely by a U.S. person or authorized foreign person and sufficient security precautions must be taken to prevent the unauthorized release of the technology. Such security precautions include encryption of the technical data, the use of secure network connections, such as virtual private networks, the use of passwords or other access restrictions on the electronic device or media on which the technical data is stored, and the use of firewalls and other network security measures to prevent unauthorized access.

(iii) The U.S. person is an employee of the U.S. government or is directly employed by a U.S. person and not by a foreign subsidiary.

(iv) Technical data authorized under this exception may not be used for foreign production purposes or for defense services unless authorized through a license or other approval.

(v) The U.S. employer of foreign persons must document the use of this exemption by foreign person employees,

including the reason that the technical data is needed by the foreign person for their temporary business activities abroad on behalf of the U.S. person.

(vi) Classified information is sent or taken outside the United States in accordance with the requirements of the Department of Defense National Industrial Security Program Operating Manual (unless such requirements are in direct conflict with guidance provided by the Directorate of Defense Trade Controls, in which case such guidance must be followed).

* * *

PART 127—VIOLATIONS AND PENALTIES

■ 22. The authority citation for part 127 continues to read as follows:

Authority: Sections 2, 38, and 42, 90, 90 Stat. 744 (22 U.S.C. 2752, 2778, 2791); 22 U.S.C. 401; 22 U.S.C. 2651a; 22 U.S.C. 2779a; 22 U.S.C. 2780; E.O. 13637, 78 FR 16129.

■ 23. Section 127.1 is amended by adding paragraphs (a)(6) and (b)(4) to read as follows:

§ 127.1 Violations.

(a) * * *

(6) To export, reexport, retransfer, or otherwise make available to the public technical data or software if such person has knowledge that the technical data or software was made publicly available without an authorization described in § 120.11(b) of this subchapter.

(b) * * *

(4) To release or otherwise transfer information, such as decryption keys, network access codes, or passwords, that would allow access to other technical data in clear text or to software that will result, directly or indirectly, in an unauthorized export, reexport, or retransfer of the technical data in clear text or software. Violation of this provision will constitute a violation to the same extent as a violation in connection with the export of the controlled technical data or software.

* * *

Dated: May 20, 2015.

Rose E. Gottenmoeller,

Under Secretary, Arms Control and International Security, Department of State.

[FR Doc. 2015-12844 Filed 6-2-15; 8:45 am]

BILLING CODE 4710-25-P

DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT

24 CFR Parts 91 and 576

[Docket No. FR-5474-N-02]

RIN 2506-AC29

Emergency Solutions Grants (ESG) Program, Solicitation of Comment on Specific Issues

AGENCY: Office of the Assistant Secretary for Community Planning and Development, HUD.

ACTION: Regulatory review; request for comments.

SUMMARY: On December 5, 2011, HUD published an interim rule entitled "Homeless Emergency Assistance and Rapid Transition to Housing: Emergency Solutions Grants Program and Consolidated Plan Conforming Amendments" (interim rule). The comment period for the interim rule ended on February 3, 2012. Because recipients and subrecipients have now had more experience implementing the interim rule, HUD recognizes that they may have additional input and comments for HUD to consider in its development of the ESG final rule (final rule). Therefore, this document takes comments for 60 days to allow additional time for public input, and for HUD to solicit specific comment on certain issues.

DATES: *Comment due date:* August 3, 2015.

ADDRESSES: Interested persons are invited to submit comments responsive to this request for information to the Regulations Division, Office of General Counsel, Department of Housing and Urban Development, 451 7th Street SW., Room 10276, Washington, DC 20410-7000. Communications must refer to the above docket number and title and should contain the information specified in the "Request for Comments" of this notice.

Electronic Submission of Comments. Interested persons may submit comments electronically through the Federal eRulemaking Portal at <http://www.regulations.gov>. HUD strongly encourages commenters to submit comments electronically. Electronic submission of comments allows the commenter maximum time to prepare and submit a comment, ensures timely receipt by HUD, and enables HUD to make them immediately available to the public. Comments submitted electronically through the <http://www.regulations.gov> Web site can be viewed by interested members of the public. Commenters should follow

instructions provided on that site to submit comments electronically.

Submission of Hard Copy Comments. Comments may be submitted by mail or hand delivery. To ensure that the information is fully considered by all of the reviewers, each commenter submitting hard copy comments, by mail or hand delivery, should submit comments or requests to the address above, addressed to the attention of the Regulations Division. Due to security measures at all federal agencies, submission of comments or requests by mail often result in delayed delivery. To ensure timely receipt of comments, HUD recommends that any comments submitted by mail be submitted at least 2 weeks in advance of the public comment deadline. All hard copy comments received by mail or hand delivery are a part of the public record and will be posted to <http://www.regulations.gov> without change.

Note: To receive consideration as public comments, comments must be submitted through one of the two methods specified above. Again, all submissions must refer to the docket number and title of the rule.

No Facsimile Comments. Facsimile (fax) comments are not acceptable.

Public Inspection of Comments. All comments submitted to HUD regarding this notice will be available, without charge, for public inspection and copying between 8 a.m. and 5 p.m. weekdays at the above address. Due to security measures at the HUD Headquarters building, an advance appointment to review the documents must be scheduled by calling the Regulation Division at 202-708-3055 (this is not a toll-free number). Copies of all comments submitted will also be available for inspection and downloading at <http://www.regulations.gov>.

FOR FURTHER INFORMATION CONTACT:

Norm Suchar, Director, Office of Special Needs Assistance Programs, Office of Community Planning and Development, Department of Housing and Urban Development, 451 7th Street SW., Room 7262, Washington, DC 20410-7000, telephone number (202) 708-4300 (this is not a toll-free number). Persons with hearing or speech impairments may access this number through TTY by calling the toll-free Federal Relay Service at 800-877-8339.

SUPPLEMENTARY INFORMATION:

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
AUSTIN DIVISION

DEFENSE DISTRIBUTED and	§	Case No. 15-CV-372-RP
SECOND AMENDMENT FOUNDATION, INC.,	§	
	§	
Plaintiffs,	§	
	§	
v.	§	
	§	
U.S. DEPARTMENT OF STATE, et al.,	§	
	§	
Defendants.	§	
-----	§	

MEMORANDUM OF POINTS AND AUTHORITIES IN REPLY TO DEFENDANTS'
OPPOSITION TO PLAINTIFFS' MOTION FOR PRELIMINARY INJUNCTION

Come now Plaintiffs, Defense Distributed and Second Amendment Foundation, Inc., by
and through counsel, and submit their Memorandum of Points and Authorities in Reply to
Defendants' Opposition to Plaintiffs' Motion for Preliminary Injunction.

Dated: June 24, 2015

Respectfully submitted,

GURA & POSSESSKY, PLLC

FISH & RICHARDSON P.C.

/s/ Alan Gura

/s/ William B. Mateja

Alan Gura
Virginia Bar No. 68842*
Gura & Possessky, PLLC
105 Oronoco Street, Suite 305
Alexandria, Virginia 22314
703.835.9085 / Fax 703.997.7665
alan@gurapossessky.com

William T. "Tommy" Jacks
Texas State Bar No. 10452000
William B. Mateja
Texas State Bar No. 13185350
David S. Morris
Texas State Bar No. 24032877
FISH & RICHARDSON P.C.
One Congress Plaza, Suite 810
111 Congress Avenue
Austin, Texas 78701
(512) 472-5070 (Telephone)
(512) 320-8935 (Facsimile)
jacks@fr.com
dmorris@fr.com
mateja@fr.com

Matthew Goldstein
D.C. Bar No. 975000*
Matthew A. Goldstein, PLLC
1012 14th Street NW, Suite 620
Washington, DC 20005
202.550.0040/Fax 202.683.6679
matthew@goldsteinpllc.com

Josh Blackman
Virginia Bar No. 78292**
1303 San Jacinto Street
Houston, Texas 77002
202.294.9003/Fax: 713.646.1766
joshblackman@gmail.com

*Admitted pro hac vice

**Admission to W.D. Tex. Bar pending

Table of Contents

Table of Authorities.....	ii
Preliminary Statement.....	1
Argument.....	1
I. The Government Misstates the Relevant Legal Standards.	1
II. Defendants’ Prior Restraint Scheme is Ultra Vires.	2
III. Defendants Ignore the Realities of Internet Accessibility and Disregard Defense Distributed’s Efforts to Obtain Guidance Regarding Compliance.	4
IV. Defendants Fail to Acknowledge that Plaintiffs’ Files Are Protected Speech.....	5
V. Plaintiffs’ Speech Does Not Threaten National Security or Foreign Policy.....	7
VI. Defendants’ Censorship Causes Real, Irreparable Injury.	10
VII. Plaintiffs Have Standing to Raise Their Second Amendment Claims.....	10
VIII. Plaintiffs Will Prevail on Their Second Amendment Claims.	11
IX. Defendants’ Definition of “Export” is Unconstitutionally Overbroad.	13
X. Defendants’ Application of ITAR Is Not Content Neutral.	14
XI. Defendants’ ITAR Review Process Creates an Interminable Prior Restraint.	14
Conclusion.....	15

Table of Authorities

Cases

<i>Addis v. Zimmer, Inc.</i> , 2003 WL 22997870 (W.D. Tex. Nov. 12, 2003)	6
<i>Almazan v. CTB, Inc.</i> , 2000 WL 33348244 (W.D. Tex. Apr. 27, 2000)	6
<i>Ass’n of Am. Physicians & Surgs. v. Tex. Med. Bd., (TMB)</i> , 627 F.3d 547 (5th Cir. 2010).	11
<i>Bernstein v. U.S. Dep’t of Justice</i> , 176 F.3d 1132 (9th Cir. 1999).	5, 6
<i>Boumediene v. Bush</i> , 553 U.S. 723 (2008).	14
<i>Carey v. Pop. Servs. Int’l</i> , 431 U.S. 678 (1977)	11
<i>CFTC v. Vartuli</i> , 228 F.3d 94 (2d Cir. 2000).	6, 7
<i>Consolidated Edison Co. of N.Y. v. Public Serv. Comm’n of N.Y.</i> , 447 U.S. 530 (1980).	14
<i>Edward J. DeBartolo Corp. v. Florida Gulf Coast Bldg. & Const. Trades Council</i> , 485 U.S. 568 (1988)	13
<i>Employment Div., Dep’t of Human Res. of Or. v. Smith</i> , 494 U.S. 872 (1990).	12
<i>Ezell v. City of Chicago</i> , 651 F.3d 684 (7th Cir. 2011).	10
<i>Faculty Senate of Fla. Int’l U. v. Winn</i> , 477 F. Supp. 2d 1198 (S.D. Fla. 2007).	10
<i>FDIC v. Meyer</i> , 510 U.S. 471 (1994).	3
<i>Junger v. Daley</i> , 209 F.3d 481 (6th Cir. 2000).	5, 6

<i>Mance v. Holder</i> , No. 4:14-cv-539-O, 2015 U.S. Dist. LEXIS 16679 (N.D. Tex. Feb. 11, 2015).	11
<i>N.L.R.B. v. Catholic Bishop of Chicago</i> , 440 U.S. 490 (1979)	13
<i>Nat’l Fed. Of the Blind of Texas, Inc. v. Abbott</i> , 647 F.3d 202 (5th Cir. 2011).	2
<i>New Orleans Depot Servs., Inc. v. Director, Office of Worker’s Compensation Programs</i> , 718 F.3d 384 (5th Cir. 2013).	3
<i>New York Times v. United States</i> , 403 U.S. 713 (1971)	7, 13
<i>Rasul v. Myers</i> , 563 F.3d 527 (D.C. Cir. 2009)	14
<i>Reed v. Gilbert</i> , 2015 WL 2473374 (U.S. June 18, 2015).	14
<i>Reid v. Covert</i> , 354 U.S. 1 (1957).	13
<i>Reliable Consultants, Inc. v. Earle</i> , 517 F.3d 738 (5th Cir. 2008).	11
<i>Roberts v. U.S. Jaycees</i> , 468 U.S. 609 (1984).	12
<i>United States v. Carter</i> , 549 F. Supp. 2d 1257 (D. Nev. 2008).	5
<i>United States v. Chi Mak</i> , 683 F.3d 1126 (9th Cir. 2012).	9
<i>United States v. Edler Indus.</i> , 579 F.2d 516 (9th Cir. 1978)	3
<i>United States v. Mead Corp.</i> , 533 U.S. 218 (2001).	4
<i>Universal City Studios, Inc. v. Corley</i> , 273 F.3d 429 (2d Cir. 2001).	6, 7

<i>Ward v. Rock Against Racism</i> , 491 U.S. 781 (1989).....	14
<i>Weste v. United States</i> , 2013 WL 2896843 (W.D. Tex. June 11, 2013).	5
<i>Wrenn v. District of Columbia</i> , 2015 WL 3477748 (D.D.C. May 18, 2015).	10
 Statutes and Rules	
18 U.S.C. § 922(p).	8
22 U.S.C. § 1934(a) (1970).	3
22 U.S.C. § 2778(a)(1)	3
Fed. R. Civ. P. 65.	1
 Other Authorities	
80 Fed. Reg. 31,525.	4
Black’s Law Dictionary (10th ed. 2014).	3

MEMORANDUM OF POINTS AND AUTHORITIES IN REPLY TO DEFENDANTS’
OPPOSITION TO PLAINTIFFS’ MOTION FOR PRELIMINARY INJUNCTION

PRELIMINARY STATEMENT

In equating the online publication of unclassified data with the export of munitions, Defendants reveal a fundamental misunderstanding of the relevant technology at issue. This misunderstanding extends to other basic facts, *e.g.*, DDTC did not merely “*suggest*[] that the technical data be removed from Defense Distributed’s website,” Opp. 5 (emphasis added)—its “Enforcement Division” instructed Plaintiff that its speech “should be removed from public access immediately.” App. 14. Defendants’ legal arguments are in the same vein, soft-peddling a radical restriction on basic rights as a plain export control regime having nothing to do with Americans’ ability to express and arm themselves in the United States. The arguments are unconvincing. Plaintiffs’ Motion for Preliminary Injunction (Dkt. 7) should be granted.

ARGUMENT

I. THE GOVERNMENT MISSTATES THE RELEVANT LEGAL STANDARDS.

Plaintiffs are puzzled by the allegation that their “failure to address the legal requirements for a preliminary injunction alone warrants the straightforward denial of their motion,” Opp. at 2, and the overheated claim that “Plaintiffs here have not even attempted to demonstrate” three of the traditional elements, *id.* The familiar test is set out on page 10, under “Summary of Argument,” and each Roman numeral under “Argument” relates to each of the standard elements, with a fifth section discussing Rule 65’s bond requirements. It is Defendants who apparently believe the standards must be manipulated to achieve the correct result.

The prohibitive/mandatory distinction test Defendants endorse is inapposite. While a mandatory injunction is more difficult to obtain than a prohibitive one, two flaws undermine

Defendants' argument of this point. First, Defendants inexplicably assume that the status quo began with their decision to require pre-publication authorization. But as Plaintiffs demonstrated, requiring pre-publication approval of Internet speech is a new application of ITAR. For years, the government disclaimed ITAR's application of a prior restraint. It simply cannot be that every new regulatory action re-defines the "status quo," such that the Government gets a "mandatory" thumb on the scale in every case for injunctive relief. Moreover, the injunction requested is prohibitive, not mandatory. Plaintiffs seek to stop misconduct, not to obtain some new benefit.

Defendants also erroneously suggest that because Defense Distributed's website contains advertising, and offers the Ghost Gunner for sale, the commercial speech doctrine applies. Opp. at 16, n. 13. But Defense Distributed is a "non-profit corporation," Wilson Decl. ¶ 24, whose goal is "to publish and distribute, *at no cost to the public*, such information and knowledge on the Internet *in promotion of the public interest*." *Id.* ¶ 2 (emphasis added). Even if Plaintiffs charged for downloading the files, their speech would still be predominantly expressive. That Defense Distributed cannot afford to give away the Ghost Gunner for free, and sells the machine to fund its charitable operations, does not alter the fact that the Ghost Gunner files more than "implicitly advocate for [plaintiff's] views, ideas, goals, causes, and values." *Nat'l Fed. Of the Blind of Texas, Inc. v. Abbott*, 647 F.3d 202, 212-13 (5th Cir. 2011).

II. DEFENDANTS' PRIOR RESTRAINT SCHEME IS ULTRA VIRES.

Defendants' flawed understanding of the technology at issue guides their unconstitutional interpretation of the Arms Export Control Act ("AECA"). To the Government, posting CAD files on the Internet "would be *equivalent* to providing the defense article itself." Opp. at 7 (emphasis added). This conclusion cannot be reconciled with the AECA's plain text or intent.

Congress authorized the President "to control the import and the *export* of defense

articles and defense services and to provide foreign policy guidance to persons of the United States involved in the export and import of such articles and services.” 22 U.S.C. § 2778(a)(1) (emphasis added). The AECA does not define “export,” and, “[i]n the absence of such a definition, [courts] construe a statutory term in accordance with its ordinary or natural meaning.” *FDIC v. Meyer*, 510 U.S. 471, 476 (1994); *see also New Orleans Depot Servs., Inc. v. Director, Office of Worker’s Compensation Programs*, 718 F.3d 384, 391 (5th Cir. 2013). Defendants’ claim hinges on the court accepting its novel argument that an “export” includes public speech in the United States, not directed at a particular listener, if a foreign person can listen. This is far afield from the well-accepted, unambiguous definition of export: “[a] product or service created in one country and transported to another.” Black’s Law Dictionary (10th ed. 2014).

Defendants cite to *United States v. Edler Indus.*, 579 F.2d 516, 521 (9th Cir. 1978) for the proposition that the subject files are ITAR-controlled because Congress intended to control technical data “directly relevant to the production of a specified article on the Munitions List.” Opp. at 29. This is a red herring because Congressional intent to control “technical data” under the AECA is not at issue in this action.¹ The question of whether Plaintiffs’ public speech contains ITAR-controlled technical data is irrelevant if public speech is not considered an “export.” Moreover, it is important to note that the conduct at issue in *Edler* involved private speech, not public speech; and the *Edler* court found that, regardless of the Congressional intent to control technical data under AECA’s predecessor, the Mutual Security Act of 1954, 22 U.S.C. § 1934(a) (1970), ITAR must be narrowly applied to avoid interfering with constitutionally protected speech. *Edler Indus.*, 579 F.2d at 521. Even if the Court departs from the ordinary or

¹ See Opp. at 11 (“Plaintiffs do not suggest that Defendants lack authority under the AECA to construct a narrowly-tailored regime to regulate the export of certain technical data.”).

natural meaning of the term “export” in determining Congressional intent, the AECA is silent or ambiguous with respect to public speech. Defendants’ command to remove data from Defense Distributed’s website preceded by two years the June 3, 2015 notice of proposed rulemaking. 80 Fed. Reg. 31,525. The prepublication approval requirement’s informal imposition on a “case-by-case” basis, based on internal, unpublished guidelines, closely resembles the “ruling letters” at issue in *United States v. Mead Corp* that “respond to transactions of the moment.” 533 U.S. 218, 223 (2001); Opp. at 4 (“These assessments are made on a *case-by-case basis* through an inter-agency process, evaluating whether the article is covered by the USML”) (emphasis added). As a result, *Skidmore*, rather than *Chevron* deference is appropriate. *Id.* at 228.

Defendants’ application of ITAR to all public speech clearly exceeds permissible bounds. It is unreasonable to assume that Congress ever expected the AECA would be used to censor public speech by citizens inside the United States merely because foreign persons can listen.

III. DEFENDANTS IGNORE THE REALITIES OF INTERNET ACCESSIBILITY AND DISREGARD DEFENSE DISTRIBUTED’S EFFORTS TO OBTAIN GUIDANCE REGARDING COMPLIANCE.

Conceding that Plaintiffs may share the disputed technical data with other Americans, and that Plaintiffs may use the technical data “to make or acquire firearms in the United States,” Defendants nonetheless assert that the speech’s ordinary Internet publication would constitute an export of defense articles. Opp. at 1, 14-16. Thus, should a foreigner somehow come into contact with a file posted on the Internet for the sole audience of a U.S. person, the publisher could be subject to severe civil and criminal penalties.²

Defendants’ suggestion that their prior restraint could be avoided if Plaintiffs restricted

² Defendants offer that “no one need risk criminal prosecution or civil sanction because it is possible to get an advance determination as to” ITAR’s application. Opp. at 28. The nearly two years Plaintiff waited to resolve its commodity jurisdiction request is a long time to stay silent.

access to their files to U.S. internet protocol (“IP”) addresses, Aguirre Decl. at ¶ 16; Opp. at 1, 5, 14-15, n. 4, is naïve at best. First, as any unintentional disclosure to a foreign person is a strict liability offense under ITAR, relying on IP address filtering to keep oneself on the right side of the law is hardly prudent. Moreover, IP addresses can be faked (“spoofed”) quite easily, allowing foreign nationals to access files on the Internet domestically or abroad at Plaintiffs’ peril.³ And, even if Plaintiffs were somehow able to always limit access to domestic IP addresses, there is no way to stop a foreign person from looking at (or using) a U.S. person’s internet connection. Every embassy in Washington is steps away from free, domestic IP WiFi. And the State Department has *never before*, including in its latest proposed notice for rulemaking, offered IP filtering as an acceptable method to publish files to the Internet (much less a safe harbor). In sum, Defendants have effectively declared the Internet a forbidden ground for collaboration if a CAD file might fall within their overbroad definition of “technical data.”⁴

IV. DEFENDANTS FAIL TO ACKNOWLEDGE THAT PLAINTIFFS’ FILES ARE PROTECTED SPEECH.

Defendants give short shrift to the two leading precedents relating to First Amendment protection for computer code, *Bernstein* and *Junger*, relegating them to a sparse footnote and dubbing them the “other two cases cited by Plaintiffs.” Opp. at 13, n. 10 (citing *Bernstein v. U.S. Dep’t of Justice*, 176 F.3d 1132, 1139-43 (9th Cir. 1999); *Junger v. Daley*, 209 F.3d 481, 485 (6th Cir. 2000)). Both of these cases held—as the government must acknowledge—that

³ *Weste v. United States*, 2013 WL 2896843, at *14 (W.D. Tex. June 11, 2013); *United States v. Carter*, 549 F. Supp. 2d 1257, 1268-69 (D. Nev. 2008).

⁴ Although Defendants fault Defense Distributed for not “inquir[ing] about whether” the files could be limited to “U.S. persons within the United States,” or how “to post the technical data on the Internet without violating ITAR,” Opp. at 5, 9, 14, Defense Distributed repeatedly sought guidance on ITAR compliance to no avail. Pl. Br. at 19-20; App. 3-4, ¶¶ 10-11; Exs. 18-23.

computer code is protected by the First Amendment.⁵ Indeed, Plaintiffs' files are more expressive than *Bernstein*'s encryption algorithm or *Junger*'s source code.

Unable to challenge *Bernstein* and *Junger*'s core holding, Defendants change the facts, conflating the CAD and Ghost Gunner files in question and claiming that these are purely functional. But the two file types are distinct, and they are each expressive.⁶ Defendants' confusion is based on a declaration by one Lisa Aguirre, who appears without a curriculum vitae and whose qualifications are unknown. *Addis v. Zimmer, Inc.*, 2003 WL 22997870, at *1 (W.D. Tex. Nov. 12, 2003) (striking an expert whose report lacked a curriculum vitae); *Almazan v. CTB, Inc.*, 2000 WL 33348244, at *7 (W.D. Tex. Apr. 27, 2000) (recognizing importance of c.v. in assessing design expert's qualifications). Her declaration, based on "personal knowledge" and "information provided to [her] in [her] official capacity," mischaracterizes the technology's operation, and repeatedly conflates the commodity jurisdiction requests. Aguirre Decl. at ¶ 4. Wilson's supplemental declaration responds to Aguirre's errors. Ex. 1 at ¶¶ 37-45.

Simply stated, and as elaborated by Wilson, CAD files are not "executable," and creating the Liberator indeed "requires additional craftsmanship, know-how, tools, and materials," contrary to Aguirre's position. Aguirre Decl. ¶ 29.b; Ex. 1 at ¶¶ 4-36. This is *not* a case where "a human's mental faculties do not intercede," but rather the files "communicate information comprehensible to a human [and] qualify as speech." *Universal City Studios, Inc. v. Corley*, 273 F.3d 429, 448 (2d Cir. 2001). Accordingly, *CFTC v. Vartuli*, 228 F.3d 94 (2d Cir. 2000), upon

⁵ Contrary to the Defendants' assertion, Opp. at 13 n. 10, Plaintiffs discuss *Bernstein*'s history. Pl. Br. n. 8.

⁶ Defendants' brief discusses only the CAD, not the Ghost Gunner files, and their submissions fail to address the broader array of files Plaintiffs seek to publish. See Complaint ¶ 37.

which Defendants heavily rely, is simply inapposite. *Vartuli* concerned software-generated currency trading instructions which did not require the human mind’s intercession—users were told that they “must ‘follow the signals with no second guessing.’” *Vartuli*, 228 F.3d at 111. In contrast, Defense Distributed’s software files, which are open-source for philosophical reasons, invite the user’s mind to intercede, modify and customize the code and any related construction of a gun or gun part. Ex. 1 at ¶ 46.

Importantly, the CAD files and the Ghost Gunner files can both be used in the generation of a product and are expressive themselves. “[T]he fact that a program has the capacity to direct the functioning of a computer does not mean that it lacks the additional capacity to convey information, and it is the conveying of information that renders instructions ‘speech’ for purposes of the First Amendment.” *Universal City*, 273 F.3d at 447.

V. PLAINTIFFS’ SPEECH DOES NOT THREATEN NATIONAL SECURITY OR FOREIGN POLICY.

As Justice Stewart recognized in the “Pentagon Papers” case, a prior restraint is justified only where the disclosure will “surely result in *direct, immediate, and irreparable* damage to our Nation or its people.” *New York Times v. United States*, 403 U.S. 713, 730 (1971) (Stewart, J., concurring) (emphasis added). Defendants’ alleged national security and foreign policy harms are indirect, indeterminate, and speculative. They do not even come close to meeting the threshold identified by the Supreme Court in the Pentagon Papers case, where the national security implications were far more concrete and actionable than anything identified in this case.

Defendants’ claim of national security and foreign policy harms centers around the notion that the Liberator’s design allows the creation of “a lethal firearm that can be easily modified to be virtually undetectable in metal detectors and other security equipment.” Opp. at 10 (citing Aguirre Decl. at ¶ 35); Aguirre Decl. at n. 9. But just about any firearm, in the wrong

hands, can theoretically threaten national security. Could Defendants banish *all* firearms-related speech from the Internet by asserting “national security?” And why stop with firearms?

Countless technologies may be repurposed by a foreign military.

In any event, Defendants again show a fundamental misunderstanding of the relevant technology, ignoring the fact that one of the modifications required to render the Liberator “undetectable by metal detectors”—the removal of the steel firing pin component—also renders it a paperweight.⁷ Ex. 1 at 33. Furthermore, its substantial physical size and obvious appearance as a firearm or firearm component (complete with a trigger guard and handgrip) render it readily detectable by X-ray machines, millimeter wave machines, pat-downs, and physical bag searches. Of course, as noted *supra*, Aguirre has not been proffered as an expert in firearms functionality, nor is there any evidence that she could qualify as one.

Moreover, assuming, *arguendo*, that the Liberator, as designed, could somehow be converted into a working, undetectable gun, the design itself is not for an undetectable (i.e., illegal, per 18 U.S.C. § 922(p)) firearm. *Id.* at ¶¶ 14, 33. Just as a long-barreled shotgun is not regulated under the National Firearms Act because it might be sawed off with a hacksaw, the constitutionally-protected sharing of the Liberator files on domestic web sites should not be restrained based on the speculative (and false) theory that someone could remove all of the metal components from it and still have a functioning firearm. Moreover, plans and instructions for building much more easily concealable (though equally capable of firing projectiles) devices such as pen guns or “zip” guns are widely available in books and on Internet forums.

The other items for which Plaintiffs have submitted commodity jurisdiction requests are

⁷ For that matter, bullets are detectable.

similarly unlikely to create a threat to national security. For example, files substantially similar to Defense Distributed's AR-15 lower CAD files have long been hosted online by other individuals and organizations. App. 283-84. The alleged risk associated with the online posting of the "80% AR-15 lower receiver" Ghost Gunner CNC file Defendants identified as subject to the ITAR (App. 280-81) is even more attenuated, as the Internet is replete with downloadable CAD files for complete (as opposed to "80%" complete) AR-15 lower receivers.

Defendants rely heavily on *United States v. Chi Mak*, 683 F.3d 1126 (9th Cir. 2012), in pressing their "national security" shibboleth, but that case—involving the sharing of stolen military secrets—is wholly inapposite. *Chi Mak*'s China-bound CD containing encrypted "export-controlled naval technology," 683 F.3d at 1131, was not public speech, and the defendant was not a public speaker. In contrast, Plaintiffs seek to publish information lawfully possessed by them on the Internet. Notably, the *Chi Mak* court instructed the jury that the Government bore the burden of proving that the contested technical data was not in the public domain. *Id.* at 1132.

Here, in contrast, it is obvious that for many months (and, in some cases, for years), Defendants have been aware of other examples of online sharing of other CAD files for firearm and firearm component designs, and they have done nothing to stop such publication.⁸ The CAD files for the Liberator itself remain available on the Internet (though not through Defense Distributed). Moreover, given the rapid development and availability of 3D scanners, including ones interfacing directly with 3D printers, it is difficult to see what safety gains, if any, might come from restricting Plaintiffs' fundamental liberties in this case. Wilson Supp. Decl., ¶ 48.

⁸ App. 211-12, 283-84. Aguirre's claim that existing material identified as being in the public domain did not contain CAD files, Aguirre Decl. ¶ 29(c), is thus particularly baffling.

VI. DEFENDANTS' CENSORSHIP CAUSES REAL, IRREPARABLE INJURY.

Defendants are entirely too dismissive of the fact that each additional day that passes without relief being granted is an additional day in which Americans' free speech is stifled and the right to keep and bear arms for self-defense is infringed. There is no serious dispute that, as a matter of law, the public interest in protecting First and Second Amendment freedoms will be irreparably harmed. *See Ezell v. City of Chicago*, 651 F.3d 684, 699 (7th Cir. 2011); *Wrenn v. District of Columbia*, 2015 WL 3477748 at *9 (D.D.C. May 18, 2015). Defendants' reliance on *Faculty Senate of Fla. Int'l U. v. Winn*, 477 F. Supp. 2d 1198 (S.D. Fla. 2007), for the proposition that "limits on foreign academic research" do not cause irreparable First Amendment harm, is spurious. The case involved the loss of travel funding, and the court merely applied the familiar rule that money damages are not irreparable, but compensable. Had the Government actually barred academic research, the opinion would have doubtless read very differently.

Defendants audaciously use their own two years of bureaucratic delay to argue that Plaintiffs have waited too long to seek relief. Opp. at 8-9. But Plaintiffs jumped through every hoop Defendants asked them to jump through, spending time and money in a good faith effort to comply with Defendants' ambiguous, interminable regime. This lawsuit was filed on May 6, 2015, only 21 days after Defendants' April 15, 2015 response to Defense Distributed's Ghost Gunner commodity jurisdiction requests, barring distribution of the Ghost Gunner files.

VII. PLAINTIFFS HAVE STANDING TO RAISE THEIR SECOND AMENDMENT CLAIMS.

Defendants do not question Plaintiffs' standing to raise their First and Fifth Amendment claims, assailing only Plaintiffs' Second Amendment standing on grounds that they do not, themselves, seek to manufacture arms. But they have no real response to the simple fact that "vendors and those in like positions . . . have been uniformly permitted to resist efforts at

restricting their operations by acting as advocates for the rights of third parties who seek access to their market or function,” *Carey v. Pop. Servs. Int’l*, 431 U.S. 678, 684 (1977) (quotation omitted); *Reliable Consultants, Inc. v. Earle*, 517 F.3d 738, 743 (5th Cir. 2008); *Mance v. Holder*, No. 4:14-cv-539-O, 2015 U.S. Dist. LEXIS 16679, at *25 n.8 (N.D. Tex. Feb. 11, 2015).

To the extent it was not obvious to the Government, from the first set of declarations, that Plaintiffs’ members, customers and visitors want to access the files for the purpose of manufacturing firearms for self-defense, that much is now made clear in the supplemental declarations. The attacks on SAF’s associational standing are spurious. SAF easily meets the test for associational standing. Its members who have unambiguously declared their intent to download files from Defense Distributed and SAF’s websites are barred from accessing files, are injured, and would thus “[a] otherwise have standing to sue in their own right; (b) the interests it seeks to protect are germane to the organization’s purpose; and (c) neither the claim asserted nor the relief requested requires the participation of individual members in the lawsuit.” *Id.*; *Ass’n of Am. Physicians & Surgs. v. Tex. Med. Bd.*, (TMB), 627 F.3d 547, 550 (5th Cir. 2010).

VIII. PLAINTIFFS WILL PREVAIL ON THEIR SECOND AMENDMENT CLAIMS.

As is often the case, the Government asserts a (specious) standing defense because it lacks any meaningful defense on the merits. Remarkably, there is no real answer to the Second Amendment claim *actually made* by the Plaintiffs. Defendants expend a great deal of effort arguing that the Second Amendment does not protect the right to export weapons. For the sake of argument, so stipulated.⁹ But Plaintiffs are not claiming the right to export weapons. Plaintiffs,

⁹Although far from the issues raised in this case, it would appear that the Government can no more bar Americans from taking guns with them overseas for the purpose of self-defense, than it can ban Americans from leaving the country with their books or religious articles.

who have the exclusive and absolute authority to define their own claims, claim the right to acquire and manufacture arms. The Government does not appear to contest that much.

Obviously, restricting the Internet publication of 3D printing and CNC files used to manufacture firearms impacts this fundamental right, and so the Government bears a heightened scrutiny burden in proving the constitutionality of its restrictions. Even were the Court to assume, for the sake of argument, that Internet publication is a form of export, it is not, like sailing a container ship into the ocean *purely* so. Is the Internet not used by American citizens, within the United States, to exchange information? Plaintiffs' Internet publication will, as intended, cause information to be delivered, received, and used domestically. However many foreign downloads Defendants might stop, banning this activity infringes Second Amendment rights within the United States.

With respect to step-two of the Second Amendment inquiry, Defendants assume without discussion that intermediate scrutiny would apply. Why? Their action impedes the exercise of core Second Amendment rights by responsible, law-abiding Americans. And even under intermediate scrutiny, Defendants barely attempt to show why such a breathtakingly radical restriction—banishing all firearms-related technical data from the Internet—would constitutionally “fit” their interests.

Indeed, the Supreme Court has recognized that when two constitutional rights work “in conjunction,” they “reinforc[e]” each other, forming a “hybrid claim.” *Employment Div., Dep’t of Human Res. of Or. v. Smith*, 494 U.S. 872, 881-82 (1990). These claims warrant “heightened scrutiny.” See *Roberts v. U.S. Jaycees*, 468 U.S. 609, 622 (1984). The first two Amendments work in tandem to protect expressive content about the right to keep and bear arms.

IX. DEFENDANTS' DEFINITION OF "EXPORT" IS UNCONSTITUTIONALLY OVERBROAD.

Defendants' surreal construction of the term "export" cannot be reconciled with the First Amendment's protection of speech that is accessible to foreign persons—even if it affects national security. Under Defendants' view, the State Department could require the *New York Times* to seek permission to "export" the Pentagon Papers—also known as publishing a newspaper—lest a foreigner read the article over the shoulder of a U.S. citizen. *Cf. New York Times*, supra, 403 U.S. 713. To avoid the constitutional difficulties with the government's interpretation of the statute, this Court should construe the meaning of "export" as narrowly as possible, excluding the infinite construction that includes sharing public information onto the Internet.¹⁰ The Government's position threatens Americans' basic freedom to communicate amongst themselves via the Internet.

Echoing its response to the Second Amendment claim, the Government remains willfully oblivious to the fact that Internet speech frequently occurs domestically, exclusively between two Americans. But also echoing its claims regarding the lack of a Second Amendment right to export arms, Defendants assert that Plaintiffs enjoy no First Amendment rights overseas. Perhaps it is not definitively clear that the Government is wrong on this claim, but close enough: "When the Government reaches out to punish a citizen who is abroad, the shield which the Bill of Rights and other parts of the Constitution provide to protect his life and liberty should not be stripped away just because he happens to be in another land." *Reid v. Covert*, 354 U.S. 1, 6 (1957)

¹⁰ *Edward J. DeBartolo Corp. v. Florida Gulf Coast Bldg. & Const. Trades Council*, 485 U.S. 568, 578 (1988) ("the section is open to a construction that obviates deciding whether a congressional prohibition of handbilling on the facts of this case would violate the First Amendment"); *N.L.R.B. v. Catholic Bishop of Chicago*, 440 U.S. 490, 500 (1979) ("an Act of Congress ought not be construed to violate the Constitution if any other possible construction remains available.").

(plurality opinion); cf. *Rasul v. Myers*, 563 F.3d 527, 531 (D.C. Cir. 2009) (per curiam). And while “practical considerations” may inform the question of what rights Americans enjoy overseas, *Boumediene v. Bush*, 553 U.S. 723, 761-62 (2008), the only relevant Americans here are on American soil.¹¹

X. DEFENDANTS’ APPLICATION OF ITAR IS NOT CONTENT NEUTRAL.

Defendants argue that strict scrutiny should not apply to ITAR’s export controls, as those controls are allegedly content-neutral. Opp. at 15. According to Defendants, their national security and foreign-policy based purpose is the controlling consideration in determining the content neutrality of the export controls in question. *Id.* (citing *Ward v. Rock Against Racism*, 491 U.S. 781, 791 (1989)). But last week’s Supreme Court decision in *Reed v. Gilbert*, 2015 WL 2473374, *8 (U.S. June 18, 2015), distinguishes *Ward*, recognizing that a government’s purpose is not relevant when a law is content-based on its face. “[A] speech regulation targeted at a specific subject matter is content based even if it does not discriminate among viewpoints within that subject matter.” 2015 WL 2473374 at *9 (citing *Consolidated Edison Co. of N.Y. v. Public Serv. Comm’n of N.Y.*, 447 U.S. 530, 537 (1980)). When a particular type of speech (or speaker) is given treatment that is different from another kind of speech (or speaker), strict scrutiny applies. *Id.* at 10-12. Here, Plaintiffs’ Internet speech is regulated based on the fact that it pertains to firearms. *Reed* clearly holds that strict scrutiny applies.

XI. DEFENDANTS’ ITAR REVIEW PROCESS CREATES AN INTERMINABLE PRIOR RESTRAINT.

In response to the charge that its imposition of ITAR on Plaintiffs creates a prior

¹¹ Defendants’ allegation that Plaintiffs’ First Amendment rights are coterminous with the threatened expressive rights of *all* third parties, Opp. at 21, is speculative. A regulation as broad and arbitrary as Defendants’ may have numerous unforeseeable applications.

restraint, Defendants respond that Defense Distributed can simply file a commodity jurisdiction request for a quick resolution of any issues. This is, at best, a rose-colored view of the process. The government casually notes that “[o]n June 21, 2013, Defense Distributed filed CJ requests for the ten items identified in the DDTC letter.” Opp. at 5. Two paragraphs, and two years later, the brief continues, “On June 4, 2015, review of Defense Distributed’s first ten requests was completed.” Opp. at 6. It was during this two-year delay that Plaintiffs’ speech rights were censored, and held in limbo. Defendants dare to suggest that Plaintiffs’ “claim of imminent irreparable injury is significantly undermined by the[] delay in seeking judicial relief.” Opp. at 8. However, not until Plaintiffs filed suit did Defendants *finally* reply to the Liberator commodity jurisdiction request. In contrast, the commodity jurisdiction request for the Ghost Gunner was resolved in only four months—shortly after this litigation commenced. The Government’s disparate processing of the commodity jurisdiction requests provides even more evidence of the content-based nature of the procedures Defendants employ in administering their prior restraint.

Aguirre claims, “in my experience, the overwhelming majority of ITAR licensing applications are approved outright or approved with conditions intended to safeguard the defense article being exported.” Aguirre Decl. at ¶ 33. However, Defendants do not identify any procedures used to review license applications for public speech. This failure is significant in light of Defense Distributed’s January 5, 2015 request for licensing guidance which, to date, Defendants have not responded to. App. 305. Even if the prepublication requirement satisfies other First Amendment concerns, the Defendants’ continued failure to provide any indicia of adequate procedures, defeats their prior restraint under both the First and Fifth Amendments.

CONCLUSION

The motion for preliminary injunction should be granted.

Dated: June 24, 2015

Respectfully submitted,

GURA & POSSESSKY, PLLC

FISH & RICHARDSON P.C.

/s/ Alan Gura

Alan Gura
Virginia Bar No. 68842*
Gura & Possessky, PLLC
105 Oronoco Street, Suite 305
Alexandria, Virginia 22314
703.835.9085 / Fax 703.997.7665
alan@gurapossessky.com

/s/ William B. Mateja

William T. "Tommy" Jacks
Texas State Bar No. 10452000
William B. Mateja
Texas State Bar No. 13185350
David S. Morris
Texas State Bar No. 24032877
FISH & RICHARDSON P.C.
One Congress Plaza, Suite 810
111 Congress Avenue
Austin, Texas 78701
(512) 472-5070 (Telephone)
(512) 320-8935 (Facsimile)
jacks@fr.com
dmorris@fr.com
mateja@fr.com

Matthew Goldstein
D.C. Bar No. 975000*
Matthew A. Goldstein, PLLC
1012 14th Street NW, Suite 620
Washington, DC 20005
202.550.0040/Fax 202.683.6679
matthew@goldsteinpllc.com

Josh Blackman
Virginia Bar No. 78292**
1303 San Jacinto Street
Houston, Texas 77002
202.294.9003/Fax: 713.646.1766
joshblackman@gmail.com

*Admitted pro hac vice

**Admission to W.D. Tex. Bar pending

Certificate of Service

The undersigned certifies that the foregoing document was filed electronically in compliance with Local Rule CV-5(a) on June 24, 2015, and was served on all counsel who are deemed to have consented to electronic service. Local Rule CV-5(b)(1). Any and all other counsel of record not deemed to have consented to electronic service were served with a true and correct copy of the foregoing by U.S. Mail and/or electronic mail on June 24, 2015.

/s/ William B. Mateja
William B. Mateja

EXHIBIT 1

FILED UNDER SEAL

SUPPLEMENTAL DECLARATION OF CODY WILSON

EXHIBIT 2

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
AUSTIN DIVISION

DEFENSE DISTRIBUTED and
SECOND AMENDMENT FOUNDATION, INC.,

Plaintiffs,

v.

U.S. DEPARTMENT OF STATE, et al.,

Defendants.

§ Case No. 15-CV-372-RP
§
§
§
§
§
§
§
§
§
§

SUPPLEMENTAL DECLARATION OF ALAN GOTTLIEB

I, Alan Gottlieb, declare:

1. I am a citizen of the United States and a resident of the state of Washington. I make this declaration as a supplement to the declaration I provided earlier for use in the above-referenced case. I make this declaration based on my personal knowledge and, if called upon to do so, could and would testify competently to the matters set forth below.

2. I am the Executive Vice President of the Second Amendment Foundation, Inc. (SAF). SAF is a non-profit membership organization incorporated under the laws of Washington with its principal place of business in Bellevue, Washington. SAF has over 650,000 members and supporters nationwide, including Texas. The purposes of SAF include education, research, publishing, and legal action focusing on the constitutional right to privately own and possess firearms, and the consequences of gun control.

3. The issues raised by, and consequences of, Defendants' policies restricting the sharing of firearms-related files over the Internet are of great interest to SAF's constituency.

Were Defense Distributed not prohibited by Defendants from sharing on the Internet its files related to lawful firearms, countless law-abiding, responsible adult SAF members and supporters would access, study, share, modify, and learn from Defense Distributed's various files, and use them to build lawful firearms for self-defense and to keep such firearms operable for self-defense. They would also do this with similar firearms-related CAD files that they or others have created. But for the threats from Defendants of criminal and civil liability, SAF members would create and share CAD files relating to lawful firearms—again, in connection with the building of lawful firearms for self-defense and with maintaining lawful firearms operable for purposes of self-defense.

4. In furtherance of SAF's mission, and to serve its members and the public, SAF would publish and promote, on the Internet, the free distribution of Defense Distributed's various files, and allow its members and others to upload their own firearm-related CAD files to SAF's servers for Internet publication, for purposes of the construction of lawful firearms for self-defense. SAF is presently refraining from doing so only owing to Defendants' interpretation of ITAR, including threats against Defense Distributed of potential criminal and civil liability.

5. SAF is proud to bring this action on behalf of its members. Conn Williamson and Peter Versnel are two of the many members of SAF.

I declare under penalty of perjury that the foregoing is true and correct.

Executed this the 23RD day of June, 2015.

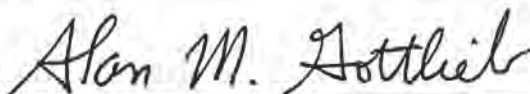

Alan Gottlieb

EXHIBIT 3

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
AUSTIN DIVISION

DEFENSE DISTRIBUTED and
SECOND AMENDMENT FOUNDATION, INC.,

Plaintiffs,

v.

U.S. DEPARTMENT OF STATE, et al.,

Defendants.

Case No. 15-CV-372-RP

SUPPLEMENTAL DECLARATION OF CONN WILLIAMSON

I, Conn Williamson, declare:

1. I am a citizen of the United States and a resident of the State of Washington. I make this declaration as a supplement to the declaration I provided earlier for use in the above-referenced case. I make this declaration based on my personal knowledge and, if called upon to do so, could and would testify competently to the matters set forth below.

2. I am a member of the Second Amendment Foundation (SAF).

3. I am not prohibited from owning lawful firearms by any local, state, or federal law, regulation, or court order.

4. But for the threats of criminal and civil liability made to Defense Distributed by the above-referenced Defendants, and those Defendants' related interpretation of ITAR, I would access online, study, share online, and learn from Defense Distributed's various firearms-related files, including files related to the Liberator handgun, as well as similar files related to firearms that Defense Distributed or others have created, for various purposes, including the manufacture and maintenance of lawful firearms that I would use for self-defense. I would access these files

via the Defense Distributed web site and via the SAF web site and download them from those sites, when posted there. I would also upload and share such files via the SAF web site, so that other United States citizens could download them and use them for constructing and maintaining lawful firearms for self-defense.

I declare under penalty of perjury that the foregoing is true and correct.

Executed this the 24 day of June, 2015.



Conn Williamson

EXHIBIT 4

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
AUSTIN DIVISION

DEFENSE DISTRIBUTED and
SECOND AMENDMENT FOUNDATION, INC.,

Plaintiffs,

V.

U.S. DEPARTMENT OF STATE, et al.,

Defendants.

Case No. 15-CV-372-RP

SUPPLEMENTAL DECLARATION OF PETER VERSNEL

I, Peter Versnel, declare:

1. I am a citizen of the United States and a resident of the State of Washington. I make this declaration as a supplement to the declaration I provided earlier for use in the above-referenced case. I make this declaration based on my personal knowledge and, if called upon to do so, could and would testify competently to the matters set forth below.

2. I am a member of the Second Amendment Foundation (SAF).


3. I am not prohibited from owning lawful firearms by any local, state, or federal law, regulation, or court order.

4. But for the threats of criminal and civil liability made to Defense Distributed by the above-referenced Defendants, and those Defendants' related interpretation of ITAR, I would access online, study, share online, and learn from Defense Distributed's various firearms-related files, including files related to the Liberator handgun, as well as similar files related to firearms that Defense Distributed or others have created, for various purposes, including the manufacture and maintenance of lawful firearms that I would use for self-defense. I would access these files

via the Defense Distributed web site and via the SAF web site and download them from those sites, when posted there. I would also upload and share such files via the SAF web site, so that other United States citizens could download them and use them for constructing and maintaining lawful firearms for self-defense.

I declare under penalty of perjury that the foregoing is true and correct.

Executed this the 19 day of June, 2015.


Peter Versnel

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
AUSTIN DIVISION

DEFENSE DISTRIBUTED, ET AL.,	§	
	§	
Plaintiffs,	§	
	§	
V.	§	1-15-CV-372 RP
	§	
UNITED STATES DEPARTMENT OF	§	
STATE, ET AL.,	§	
	§	
Defendants.	§	

ORDER

Before the Court are Plaintiffs’ Motion for Preliminary Injunction, filed May 11, 2015 (Clerk’s Dkt. #7), Memorandum of Points and Authorities in Support of Plaintiffs’ Motion for Preliminary Injunction, filed May 11, 2015 (Clerk’s Dkt. #8) and the responsive pleadings thereto. The Court conducted a hearing on the motion on July 6, 2015. Having considered the motion, responsive pleadings, record in the case, and the applicable law, the Court is of the opinion that Plaintiffs’ motion for a preliminary injunction should be denied. See FED. R. CIV. P. 65(b).

I. BACKGROUND

Plaintiffs Defense Distributed and the Second Amendment Foundation (“SAF”) bring this action against defendants the United States Department of State, Secretary of State John Kerry, the Directorate of Defense Trade Controls (“DDTC”), and employees of the DDTC in their official and individual capacities, challenging implementation of regulations governing the “export” of “defense articles.”

Under the Arms Export Control Act (“AECA”), “the President is authorized to control the import and the export of defense articles and defense services” and to “promulgate regulations for the import and export of such articles and services.” 22 U.S.C. § 2778(a)(1). The AECA imposes both civil and criminal penalties for violation of its provisions and implementing regulations,

including monetary fines and imprisonment. *Id.* § 2278(c) & (e). The President has delegated his authority to promulgate implementing regulations to the Secretary of State. Those regulations, the International Traffic in Arms Regulation (“ITAR”), are in turn administered by the DDTTC and its employees. 22 C.F.R. 120.1(a).

The AECA directs that the “defense articles” designated under its terms constitute the United States “Munitions List.” 22 U.S.C. § 2278(a)(1). The Munitions List “is not a compendium of specific controlled items,” rather it is a “series of categories describing the kinds of items” qualifying as “defense articles.” *United States v. Zhen Zhou Wu*, 711 F.3d 1, 12 (1st Cir.) *cert. denied sub nom. Yufeng Wei v. United States*, 134 S. Ct. 365 (2013). Put another way, the Munitions List contains “attributes rather than names.” *United States v. Pulungan*, 569 F.3d 326, 328 (7th Cir. 2009) (explaining “an effort to enumerate each item would be futile,” as market is constantly changing). The term “defense articles” also specifically includes “technical data recorded or stored in any physical form, models, mockups or other items that reveal technical data directly relating to items designated in” the Munitions List. 22 C.F.R. § 120.6

A party unsure about whether a particular item is a “defense article” covered by the Munitions List may file a “commodity jurisdiction” request with the DDTTC. See 22 C.F.R. § 120.4 (describing process). The regulations state the DDTTC “will provide a preliminary response within 10 working days of receipt of a complete request for commodity jurisdiction.” *Id.* § 120.4(e). If a final determination is not provided after 45 days, “the applicant may request in writing to the Director, Office of Defense Trade Controls Policy that this determination be given expedited processing.” *Id.*

According to Plaintiffs, Defense Distributed publishes files on the Internet as a means of fulfilling its primary missions to promote the right to keep and bear arms and to educate the public, as well as generating revenue. Specifically, in December 2012 Defense Distributed made available for free on the Internet privately generated technical information regarding a number of gun-related

items (the “Published Files”). (Compl. ¶¶ 22-24). Plaintiffs allege that, on May 8, 2013, Defendants sent Defense Distributed a letter stating:

DTCC/END is conducting a review of technical data made publicly available by Defense Distributed through its 3D printing website, DEFCAD.org, the majority of which appear to be related to items in Category I of the [Munitions List]. Defense Distributed may have released ITAR-controlled technical data without the required prior authorization from the Directorate of Defense Trade Controls (DDTC), a violation of the ITAR.

(*Id.* ¶ 25).

Plaintiffs state they promptly removed the Published Files from the Internet. Further, per instruction in the May 2013 letter, Plaintiffs submitted commodity jurisdiction requests covering the Published Files on June 21, 2013. According to Plaintiffs, they have not received a response to the requests from Defendants. (*Id.* ¶¶ 26-29).

Plaintiffs further allege that, on September 25, 2014, Defense Distributed sent a request for prepublication approval for public release of files containing technical information on a machine named the “Ghost Gunner” that can be used to manufacture a variety of items, including gun parts (the “Ghost Gunner Files”).¹ Following resubmission of the request, on April 13, 2015, DDTC determined that the Ghost Gunner machine, including the software necessary to build and operate the Ghost Gunner machine, is not subject to ITAR, but that “software, data files, project files, coding, and models for producing a defense article, to include 80% AR-15 lower receivers, are subject to the jurisdiction of the Department of State in accordance with [ITAR].” (*Id.* ¶¶ 28-33).

In addition, Plaintiffs allege that since September 2, 2014, Defense Distributed has made multiple requests to DOPSR for prepublication review of certain computer-aided design (“CAD”) files. In December 2014, DOPSR informed Defense Distributed that it refused to review the CAD files. The DOPSR letter directed Defense Distributed to the DDTC Compliance and Enforcement

¹ According to Plaintiffs, Defendants identify the Department of Defense Office of Prepublication Review and Security (“DOPSR”) as the government agency from which private persons must obtain prior approval for publication of privately generated technical information subject to ITAR control. (Compl. ¶ 28).

Division for further questions on public release of the CAD files. Defense Distributed has sought additional guidance on the authorization process, but to date, Defendants have not responded. (*Id.* ¶¶ 34-36).

Plaintiffs filed this action on April 29, 2015, raising five separate claims. Specifically, Plaintiffs assert that the imposition by Defendants of a prepublication approval requirement for “technical data” related to “defense articles” constitutes: (1) an ultra vires government action; (2) a violation of their rights to free speech under the First Amendment; (3) a violation of their right to keep and bear arms under the Second Amendment; and (4) a violation of their right to due process of law under the Fifth Amendment. Plaintiffs also contend the violations of their constitutional rights entitled them to monetary damages under *Bivens v. Six Unknown Named Agents of the Federal Bureau of Narcotics*, 403 U.S. 388 (1971). Plaintiffs now seek a preliminary injunction enjoining the enforcement of any prepublication approval requirement against unclassified information under the ITAR, specifically including all files Defense Distributed has submitted for DOPSR review. The parties have filed responsive pleadings. The Court conducted a hearing on July 6, 2015 and the matter is now ripe for review.

II. STANDARD OF REVIEW

A preliminary injunction is an extraordinary remedy and the decision to grant a preliminary injunction is to be treated as the exception rather than the rule. *Valley v. Rapides Parish Sch. Bd.*, 118 F.3d 1047, 1050 (5th Cir. 1997). The party seeking a preliminary injunction may be granted relief *only* if the moving party establishes: (1) a substantial likelihood of success on the merits; (2) a substantial threat that failure to grant the injunction will result in irreparable injury; (3) that the threatened injury out-weighs any damage that the injunction may cause the opposing party; and (4) that the injunction will not disserve the public interest. See *Hoover v. Morales*, 146 F.3d 304, 307 (5th Cir.1998); *Wenner v. Texas Lottery Comm’n*, 123 F.3d 321, 325 (5th Cir. 1997); *Cherokee*

Pump & Equip. Inc. v. Aurora Pump, 38 F.3d 246, 249 (5th Cir. 1994). To show a substantial likelihood of success, “the plaintiff must present a prima facie case, but need not prove that he is entitled to summary judgment.” *Daniels Health Sciences, L.L.C. v. Vascular Health Sciences, L.L.C.*, 710 F.3d 579, 582 (5th Cir. 2013). See also *Janvey v. Alguire*, 647 F.3d 585, 596 (5th Cir. 2011) (same, citing CHARLES ALAN WRIGHT, ARTHUR R. MILLER, MARY KAY KANE, 11A FEDERAL PRACTICE & PROCEDURE § 2948.3 (2d ed. 1995) (“All courts agree that plaintiff must present a prima facie case but need not show that he is certain to win.”)). The party seeking a preliminary injunction must clearly carry the burden of persuasion on all four requirements to merit relief. *Mississippi Power & Light Co.*, 760 F.2d 618, 621 (5th Cir. 1985).

III. ANALYSIS

Defendants maintain Plaintiffs have not established any of the four requirements necessary to merit grant of a preliminary injunction. Plaintiffs, of course, disagree. The Court will briefly address the parties’ arguments concerning the final three requirements before turning to the core, and dispositive question, whether Plaintiffs have shown a likelihood of success on the merits of their claims.

A. Injury and Balancing of Interests

Defendants suggest Plaintiffs’ contention that they face irreparable injury absent immediate relief is rebutted by their delay in filing this lawsuit. However, the Supreme Court has stated that the “loss of First Amendment freedoms, for even minimal periods of time, unquestionably constitutes irreparable injury.” *Elrod v. Burns*, 427 U.S. 347, 373 (1976); see also *Palmer v. Waxahachie Indep. Sch. Dist.*, 579 F.3d 502, 506 (5th Cir. 2009) (the “loss of First Amendment freedoms for even minimal periods of time constitutes irreparable injury justifying the grant of a preliminary injunction.”). The Second Amendment protects “similarly intangible and unquantifiable interests” and a deprivation is thus considered irreparable. *Ezell v. City of Chicago*, 651 F.3d 684,

699 (7th Cir. 2011) (“for some kinds of constitutional violations, irreparable harm is presumed”). The Court thus has little trouble concluding Plaintiffs have shown they face a substantial threat of irreparable injury.

The Court has much more trouble concluding Plaintiffs have met their burden in regard to the final two prongs of the preliminary injunction inquiry. Those prongs require weighing of the respective interests of the parties and the public. Specifically, that the threatened injury out-weighs any damage that the injunction may cause the opposing party and that the injunction will not disserve the public interest. In this case, the inquiry essentially collapses because the interests asserted by Defendants are in the form of protecting the public by limiting access of foreign nationals to “defense articles.”

Plaintiffs rather summarily assert the balance of interests tilts in their favor because “[I]t is always in the public interest to prevent the violation of a party’s constitutional rights.” *Awad v. Ziriax*, 670 F.3d 1111, 1132 (10th Cir. 2012); *see also Jackson Women’s Health Org. v. Currier*, 760 F.3d 448, 458 n.9 (5th Cir. 2014) (district court did not abuse its discretion in finding injunction would not disserve public interest because it will prevent constitutional deprivations). They further assert that an injunction would not bar Defendants from controlling the export of classified information.

The Court finds neither assertion wholly convincing. While Plaintiffs’ assertion of a public interest in protection of constitutional rights is well-taken, it fails to consider the public’s keen interest in restricting the export of defense articles. *See Winter v. Natural Res. Def. Council, Inc.*, 555 U.S. 7, 24-25 (2008) (discussing failure of district court to consider injunction’s adverse impact on public interest in national defense); *Am. Civil Liberties Union v. Clapper*, 785 F.3d 787, 826 (2nd Cir. 2015) (characterizing maintenance of national security as “public interest of the highest order”). It also fails to account for the interest – and authority – of the President and Congress in matters of foreign policy and export. *See Haig v. Agee*, 453 U.S. 280, 292 (1981) (matters relating to

conduct of foreign relations “are so exclusively entrusted to the political branches of government as to be largely immune from judicial inquiry or interference”); *United States v. Pink*, 315 U.S. 203, 222–23 (1942) (conduct of foreign relations “is committed by the Constitution to the political departments of the Federal Government”); *Spectrum Stores, Inc. v. Citgo Petroleum Corp.*, 632 F.3d 938, 950 (5th Cir. 2011) (matters implicating foreign relations and military affairs generally beyond authority of court’s adjudicative powers).

As to Plaintiff’s second contention, that an injunction would not bar Defendants from controlling the export of classified information, it is significant that Plaintiffs maintain the posting of files on the Internet for free download does not constitute “export” for the purposes of the AECA and ITAR. But Defendants clearly believe to the contrary. Thus, Plaintiffs’ contention that the grant of an injunction permitting them to post files that Defendants contend are governed by the AECA and ITAR would not bar Defendants from controlling “export” of such materials stand in sharp contrast to Defendants’ assertion of the public interest. The Court thus does not believe Plaintiffs have met their burden as to the final two prongs necessary for granting Plaintiffs a preliminary injunction. Nonetheless, in an abundance of caution, the Court will turn to the core of Plaintiffs’ motion for a preliminary injunction, whether they have shown a likelihood of success on their claims

B. Ultra Vires

Plaintiffs first argue Defendants are acting beyond the scope of their authority in imposing a prepublication requirement on them under the AECA. A federal court has no subject matter jurisdiction over claims against the United States unless the government waives its sovereign immunity and consents to suit. *Danos v. Jones*, 652 F.3d 577, 581 (5th Cir. 2011) (citing *FDIC v. Meyer*, 510 U.S. 471, 475 (1994)). The ultra vires exception to sovereign immunity provides that “where the officer’s powers are limited by statute, his actions beyond those limitations are considered individual and not sovereign actions,” or “ultra vires his authority,” and thus not

protected by sovereign immunity. *Larson v. Domestic & Foreign Commerce Corp.*, 337 U.S. 682, 689 (1949). To fall within the ultra vires exception to sovereign or governmental immunity, a plaintiff must “do more than simply allege that the actions of the officer are illegal or unauthorized.” *Danos*, 652 F.3d at 583. Rather, the complaint must allege facts sufficient to establish that the officer was acting “without any authority whatever,” or without any “colorable basis for the exercise of authority.” *Id.* (quoting *Pennhurst State Sch. & Hosp. v. Halderman*, 465 U.S. 89, 101 n.11 (1984)).

The statute at issue provides:

In furtherance of world peace and the security and foreign policy of the United States, the President is authorized to control the import and the export of defense articles and defense services and to provide foreign policy guidance to persons of the United States involved in the export and import of such articles and services. The President is authorized to designate those items which shall be considered as defense articles and defense services for the purposes of this section and to promulgate regulations for the import and export of such articles and services.

22 U.S.C. § 2778(a)(1). “Export” is defined, in pertinent part, as including “[d]isclosing (including oral or visual disclosure) or transferring technical data to a foreign person whether in the United States or abroad.” 22 C.F.R. § 120.17(a)(4). Plaintiffs argue this definition falls outside Congressional intent in authorizing restriction of export of defense articles because, as interpreted by Defendants, it includes public speech within the United States.

Notably, Plaintiffs do not suggest Defendants lack authority under the AECA to regulate export of defense articles. Further, under the AECA, decisions are required to

take into account whether the export of an article would contribute to an arms race, aid in the development of weapons of mass destruction, support international terrorism, increase the possibility of outbreak or escalation of conflict, or prejudice the development of bilateral or multilateral arms control or nonproliferation agreements or other arrangements.

22 U.S.C. § 2778(a)(2). Defense Distributed admits its purpose is “facilitating *global* access to, and the collaborative production of, information and knowledge related to the three-dimensional (“3D”) printing of arms.” (Compl. ¶ 1) (emphasis added). Facilitating global access to firearms

undoubtedly “increase[s] the possibility of outbreak or escalation of conflict.” Defense Distributed, by its own admission, engages in conduct which Congress authorized Defendants to regulate. Plaintiffs have not, therefore, shown Defendants are acting without any “colorable basis for the exercise of authority.” Accordingly, they have not shown a likelihood of success on their ultra vires challenge.

C. First Amendment

Plaintiffs next argue Defendants’ interpretation of the AECA violates their First Amendment right to free speech. In addressing First Amendment claims, the first step is to determine whether the claim involves protected speech, the second step is to identify the nature of the forum, and the third step is to assess whether the justifications for exclusion from the relevant forum satisfy the requisite standard. *Cornelius v. NAACP Legal Defense & Educ. Fund, Inc.*, 473 U.S. 788, 797 (1985).

As an initial matter, Defendants argue the computer files at issue do not constitute speech and thus no First Amendment protection is afforded. First Amendment protection is broad, covering “works which, taken as a whole, have serious literary, artistic, political, or scientific value, regardless of whether the government or a majority of the people approve of the ideas these works represent.” *Miller v. California*, 413 U.S. 15, 34 (1973). *See also Brown v. Entm’t Merchants Ass’n*, 131 S. Ct. 2729, 2733 (2011) (video games’ communication of ideas and social messages suffices to confer First Amendment protection). Defendants, however, maintain the computer files at the heart of this dispute do not warrant protection because they consist merely of directions to a computer. In support, they rely on a Second Circuit opinion which held that computer instructions that “induce action without the intercession of the mind or the will of the recipient” are not constitutionally protected speech. *Commodity Futures Trading Comm’n v. Vartuli*, 228 F.3d 94, 111 (2nd Cir. 2000).

As Plaintiffs point out, one year later, the Second Circuit addressed the issue of whether computer code constitutes speech at some length in *Universal City Studios, Inc. v. Corley*, 273 F.3d 429 (2nd Cir. 2001).² The court made clear the fact that computer code is written in a language largely unintelligible to people was not dispositive, noting Sanskrit was similarly unintelligible to many, but a work written in that language would nonetheless be speech. Ultimately, the court concluded “the fact that a program has the capacity to direct the functioning of a computer does not mean that it lacks the additional capacity to convey information, and it is the conveying of information that renders instructions ‘speech’ for purposes of the First Amendment.” *Id.* at 447 (discussing other examples of “instructions” which qualified as speech under First Amendment). Similarly, the Sixth Circuit has found “[b]ecause computer source code is an expressive means for the exchange of information and ideas about computer programming . . . it is protected by the First Amendment,” even though such code “has both an expressive feature and a functional feature.” *Junger v. Daley*, 209 F.3d 481, 485 (6th Cir. 2000).

Although the precise technical nature of the computer files at issue is not wholly clear to the Court, Plaintiffs made clear at the hearing that Defense Distributed is interested in distributing the files as “open source.” That is, the files are intended to be used by others as a baseline to be built upon, altered and otherwise utilized. Thus, at least for the purpose of the preliminary injunction analysis, the Court will consider the files as subject to the protection of the First Amendment.

In challenging Defendants’ conduct, Plaintiffs urge this Court to conclude the ITAR’s imposition of a prepublication requirement constitutes an impermissible prior restraint. Prior restraints “face a well-established presumption against their constitutionality.” *Marceaux v. Lafayette City-Parish Consol. Gov’t*, 731 F.3d 488, 493 (5th Cir. 2013). See also *Organization for*

² Defendants are correct that the *Corley* court did not overrule the decision in *Vartuli*. However, the *Corley* court itself distinguished the decision in *Vartuli* as limited, because it was based on the manner in which the code at issue was marketed. That is, the defendants themselves marketed the software as intended to be used “mechanically” and “without the intercession of the mind or the will of the recipient.” *Corley*, 273 F.3d at 449 (quoting *Vartuli*, 228 F.3d at 111). Plaintiffs here have not so marketed or described the files at issue.

a *Better Austin v. Keefe*, 402 U.S. 415, 419 (1971) (“Any prior restraint on expression comes ... with a ‘heavy presumption’ against its constitutional validity”); *Shuttlesworth v. City of Birmingham*, 394 U.S. 147, 150–51 (1969) (noting “the many decisions of this Court over the last 30 years, holding that a law subjecting the exercise of First Amendment freedoms to the prior restraint of a license without narrow, objective, and definite standards to guide the licensing authority, is unconstitutional”). “[A] system of prior restraint avoids constitutional infirmity only if it takes place under procedural safeguards designed to obviate the dangers of a censorship system.” *Collins v. Ainsworth*, 382 F.3d 529, 539 (5th Cir. 2004) (quoting *Southeastern Promotions, Ltd. v. Conrad*, 420 U.S. 546, 559 (1975)).

The “heavy presumption” against constitutional validity of prior restraint is not, however, “a standard of review, and judicial decisions analyzing prior restraints have applied different standards of review depending on the restraint at issue.” *Catholic Leadership Coal. of Tex. v. Reisman*, 764 F.3d 409, 438 (5th Cir. 2014). See, e.g., *Seattle Times Co. v. Rhinehart*, 467 U.S. 20, 33 (1984) (order prohibiting dissemination of discovered information before trial “is not the kind of classic prior restraint that requires exacting First Amendment scrutiny”); *Perry v. McDonald*, 280 F.3d 159, 171 (2nd Cir. 2001) (context in which prior restraint occurs affects level of scrutiny applied);, 192 F.3d 742, 749 (7th Cir. 1999) (“We note initially that the [plaintiff] is simply wrong in arguing that all prior restraints on speech are analyzed under the same test.”).

No party suggests posting of information on the Internet for general free consumption is not a public forum. The next inquiry is thus the applicable level of protection afforded to the files at issue. Content-neutral restrictions on speech are examined under intermediate scrutiny, meaning they are permissible so long as they are narrowly tailored to serve a significant governmental interest and leave open ample alternative channels for communication of the information. *Turner Broad. Sys. v. FCC*, 520 U.S. 180, 213–14 (1997); *Ward v. Rock Against Racism*, 491 U.S. 781, 791 (1989). Content-based restrictions are examined under strict scrutiny, meaning they must be

narrowly drawn to effectuate a compelling state interest. *Perry Educ. Ass'n v. Perry Local Educators' Ass'n*, 460 U.S. 37, 46 (1983).

Not surprisingly, the parties disagree as to whether the ITAR imposes content-based restrictions. “Government regulation of speech is content based if a law applies to particular speech because of the topic discussed or the idea or message expressed.” *Reed v. Town of Gilbert*, 135 S. Ct. 2218, 2227 (2015). Plaintiffs here argue, because the regulations restrict speech concerning the entire topic of “defense articles” the regulation is content-based. “A regulation is not content-based, however, merely because the applicability of the regulation depends on the content of the speech.” *Asgeirsson v. Abbott*, 696 F.3d 454, 459 (5th Cir. 2012). Rather, determination of whether regulation of speech is content-based “requires a court to consider whether a regulation of speech ‘on its face’ draws distinctions based on the message a speaker conveys.” *Reed*, 135 S. Ct. at 2227. *See also Ward*, 491 U.S. at 791 (principal inquiry in determining content-neutrality, “is whether the government has adopted a regulation of speech because of disagreement with the message it conveys”).

Employing this inquiry, the Supreme Court has found regulations to be content-neutral where the regulations are aimed not at suppressing a message, but at other “secondary effects.” For example, the Supreme Court upheld a zoning ordinance that applied only to theaters showing sexually-explicit material, reasoning the regulation was content-neutral because it was not aimed at suppressing the erotic message of the speech but instead at the crime and lowered property values that tended to accompany such theaters. *Renton v. Playtime Theatres, Inc.*, 475 U.S. 41, 47–48 (1986). The Supreme Court similarly upheld a statute establishing buffer zones only at clinics that performed abortions, concluding the statute did not draw content-based distinctions as enforcement authorities had no need to examine the content of any message conveyed and the stated purpose of the statute was public safety. *McCullen v. Coakley*, 134 S. Ct. 2518, 2531 (2014) (noting violation of statute depended not “on what they say,” but “simply on where they say it”). The

Fifth Circuit has likewise found regulations content-neutral, even where the regulation governed a specific topic of speech. See *Kagan v. City of New Orleans*, 753 F.3d 560, 562 (5th Cir. 2014), *cert. denied*, 135 S. Ct. 1403 (2015) (upholding regulation requiring license for a person to charge for tours to City's points of interest and historic sites, "for the purpose of explaining, describing or generally relating the facts of importance thereto," finding regulation "has no effect whatsoever on the content of what tour guides say"); *Asgeirsson*, 696 F.3d at 461 (holding Texas' Open Meeting Act, prohibiting governmental body from conducting closed meetings during which public business or public policy over which the governmental body has supervision or control is discussed, to be content-neutral, because closed meetings: (1) prevent transparency; (2) encourage fraud and corruption; and (3) foster mistrust in government).

The ITAR, on its face, clearly regulates disclosure of "technical data" relating to "defense articles." The ITAR thus unquestionably regulates speech concerning a specific topic. Plaintiffs suggest that is enough to render the regulation content-based, and thus invoke strict scrutiny. Plaintiffs' view, however, is contrary to law. The Fifth Circuit rejected a similar test, formulated as "[a] regulatory scheme that requires the government to 'examine the content of the message that is conveyed' is content-based regardless of its motivating purpose," finding the proposed test was contrary to both Supreme Court and Fifth Circuit precedent. *Asgeirsson*, 696 F.3d at 460.

The ITAR does not regulate disclosure of technical data based on the message it is communicating. The fact that Plaintiffs are in favor of global access to firearms is not the basis for regulating the "export" of the computer files at issue. Rather, the export regulation imposed by the AECA is intended to satisfy a number of foreign policy and national defense goals, as set forth above. Accordingly, the Court concludes the regulation is content-neutral and thus subject to intermediate scrutiny. See *United States v. Chi Mak*, 683 F.3d 1126, 1135 (9th Cir. 2012) (finding the AECA and its implementing regulations are content-neutral).

The Supreme Court has used various terminology to describe the intermediate scrutiny

standard. *Compare Ward*, 491 U.S. at 798 (“a regulation of the time, place, or manner of protected speech must be narrowly tailored to serve the government's legitimate, content-neutral interests but that it need not be the least restrictive or least intrusive means of doing so”), with *Bd. of Trs. of State Univ. of N.Y. v. Fox*, 492 U.S. 469, 480 (1989) (requiring “the government goal to be substantial, and the cost to be carefully calculated,” and holding “since the State bears the burden of justifying its restrictions, it must affirmatively establish the reasonable fit we require”), and *Turner*, 520 U.S. at 189 (regulation upheld under intermediate scrutiny if it “further[s] an important or substantial governmental interest unrelated to the suppression of free speech, provided the incidental restrictions d[o] not burden substantially more speech than is necessary to further those interests”). The Court will employ the Fifth Circuit’s most recent enunciation of the test, under which a court must sustain challenged regulations “if they further an important or substantial governmental interest; if the governmental interest is unrelated to the suppression of free expression; and if the incidental restriction on alleged First Amendment freedoms is no greater than is essential to the furtherance of that interest.” *Time Warner Cable, Inc. v. Hudson*, 667 F.3d 630, 641 (5th Cir. 2012)

The Court has little trouble finding there is a substantial governmental interest in regulating the dissemination of military information. Plaintiffs do not suggest otherwise. *See Holder v. Humanitarian Law Project*, 561 U.S. 1, 28 (2010) (noting all parties agreed government's interest in combating terrorism “is an urgent objective of the highest order”). Nor do Plaintiffs suggest the government’s regulation is directed at suppressing free expression. Rather, they contend the regulations are not sufficiently tailored so as to only incidentally restrict their freedom of expression.

The only circuit to address whether the AECA and ITAR violate the First Amendment has concluded the regulatory scheme survives such a challenge. In so doing, the Ninth Circuit concluded the technical data regulations substantially advance the government’s interest, unrelated to the suppression of expression, because the regulations provide clear procedures for seeking

necessary approval. *Chi Mak*, 683 F.3d at 1135 (citing 22 C.F.R § 120.10(a) (the determination of designation of articles or services turns on whether an item is “specifically designed, developed, configured, adapted, or modified for a military application, and has significant military or intelligence applicability such that control under this subchapter is necessary”)). The Ninth Circuit also concluded the regulations were not more burdensome than necessary, noting the “ITAR makes a point to specifically exclude numerous categories from designation, such as general scientific, mathematical, or engineering papers.” *Id.* (citing *Humanitarian Law Project*, 561 U.S. at 29 (upholding material support statute against First Amendment challenge where the statute provided narrowing definitions to avoid infringing upon First Amendment interests)).³

Plaintiffs’ challenge here is based on their contention that Defendants have applied an overbroad interpretation of the term “export.” Specifically, Plaintiffs argue that viewing “export” as including public speech, including posting of information on the Internet, imposes a burden on expression which is greater than is essential to the furtherance of the government’s interest in protecting defense articles.

But a prohibition on Internet posting does not impose an insurmountable burden on Plaintiffs’ domestic communications. This distinction is significant because the AECA and ITAR do not prohibit domestic communications. As Defendants point out, Plaintiffs are free to disseminate the computer files at issue domestically in public or private forums, including via the mail or any other medium that does not provide the ability to disseminate the information internationally.

Nor is the Court convinced by Plaintiffs’ suggestion that the ban on Internet posting does not prevent dissemination of technical data outside national borders, and thus does not further the

³ The Ninth Circuit has also rejected a First Amendment challenge to the AECA’s predecessor, the Mutual Security Act of 1954. *See United States v. Edler Indus., Inc.*, 579 F.2d 516, 521 (9th Cir. 1978) (holding statute and regulations not overbroad in controlling conduct of assisting foreign enterprises to obtain military equipment and related technical expertise and licensing provisions of statute not an unconstitutional prior restraint on speech).

government's interests under the AECA. The Ninth Circuit addressed and rejected a similar suggestion, namely that the only way the government can prevent technical data from being sent to foreign persons is to suppress the information domestically as well, explaining:

This outcome would blur the fact that national security concerns may be more sharply implicated by the export abroad of military data than by the domestic disclosure of such data. Technical data that is relatively harmless and even socially valuable when available domestically may, when sent abroad, pose unique threats to national security. It would hardly serve First Amendment values to compel the government to purge the public libraries of every scrap of data whose export abroad it deemed for security reasons necessary to prohibit.

United States v. Posey, 864 F.2d 1487, 1496-97 (9th Cir. 1989).

The Court also notes, as set forth above, that the ITAR provides a method through the commodity jurisdiction request process for determining whether information is subject to its export controls. See 22 C.F.R. § 120.4 (describing process). The regulations include a ten day deadline for providing a preliminary response, as well as a provision for requesting expedited processing. 22 C.F.R. § 120.4(e) (setting deadlines). Further, via Presidential directive, the DDTC is required to “complete the review and adjudication of license applications within 60 days of receipt.” 74 Fed. Reg. 63497 (December 3, 2009). Plaintiffs thus have available a process for determining whether the speech they wish to engage in is subject to the licensing scheme of the ITAR regulations.

Accordingly, the Court concludes Plaintiffs have not shown a substantial likelihood of success on the merits of their claim under the First Amendment.

D. Second Amendment

Plaintiffs also argue the ITAR regulatory scheme violates their rights under the Second Amendment. Defendants contend Plaintiffs cannot succeed on this claim, both because they lack standing to raise it, and because the claim fails on the merits. As standing is jurisdictional, the Court will turn to that issue first.

a. Standing

Article III of the Constitution limits the jurisdiction of federal courts to cases and controversies. *United States Parole Comm'n v. Geraghty*, 445 U.S. 388, 395 (1980). “One element of the case-or-controversy requirement is that [plaintiffs], based on their complaint, must establish that they have standing to sue.” *Raines v. Byrd*, 521 U.S. 811, 818 (1997). This requirement, like other jurisdictional requirements, is not subject to waiver and demands strict compliance. *Raines*, 521 U.S. at 819; *Lewis v. Casey*, 518 U.S. 343, 349 n.1 (1996). To meet the standing requirement a plaintiff must show (1) she has suffered an “injury in fact” that is (a) concrete and particularized and (b) actual or imminent, not conjectural or hypothetical; (2) the injury is fairly traceable to the challenged action of the defendant; and (3) it is likely, as opposed to merely speculative, that the injury will be redressed by a favorable decision. *Friends of the Earth, Inc. v. Laidlaw Envtl. Servs. (TOC), Inc.*, 528 U.S. 167, 180-81 (2000); *Consol. Cos., Inc. v. Union Pacific R.R. Co.*, 499 F.3d 382, 385 (5th Cir. 2007); *Fla. Dep’t of Ins. v. Chase Bank of Tex. Nat’l Ass’n*, 274 F.3d 924, 929 (5th Cir. 2001) (citing *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560-61 (1992)). “The party invoking federal jurisdiction bears the burden of establishing these elements.” *Lujan*, 504 U.S. at 561.

Defendants correctly point out Defense Distributed is in full possession of the computer files at issue and thus cannot argue it is being prevented from exercising its rights under the Second Amendment.⁴ Plaintiffs maintain Defense Distributed nonetheless has standing because it is “entitled to assert the Second Amendment rights of [its] customers and website visitors.” (Plf. Brf. at 27). A litigant is generally limited to asserting standing only on behalf of himself. See *Kowalski v. Tesmer*, 543 U.S. 125, 129 (2004) (a party “generally must assert his own legal rights and interests, and cannot rest his claim to relief on the legal rights or interests of third parties”). The

⁴ No party addressed whether a corporation such as Defense Distributed itself possesses Second Amendment rights.

Supreme Court has recognized a limited exception when the litigant seeking third-party standing has suffered an "injury in fact" giving him a "sufficiently concrete interest" in the outcome of the issue, the litigant has a "close" relationship with the third party on whose behalf the right is asserted and there is a "hindrance" to the third party's ability to protect his own interests. *Powers v. Ohio*, 499 U.S. 400, 411 (1991).

Plaintiffs argue they meet this test, asserting Defense Distributed acts as a "vendor" or in a like position by way of offering the computer files for download to visitors of its website. See *Carey v. Population Servs. Int'l*, 431 U.S. 678, 684 (1977) ("vendors and those in like positions . . . have been uniformly permitted to resist efforts at restricting their operations by acting as advocates for the rights of third parties who seek access to their market or function"); *Reliable Consultants, Inc. v. Earle*, 517 F.3d 738, 743 (5th Cir. 2008) (Supreme Court precedent holds providers of product have standing to attack ban on commercial transactions involving product). As an initial matter, it is not at all clear that distribution of information for free via the Internet constitutes a commercial transaction.⁵ Moreover, Plaintiffs do not explain how visitors to Defense Distributed's website are hindered in their ability to protect their own interests. In fact, the presence of SAF as a plaintiff suggests to the contrary. Thus, whether Defense Distributed has standing to assert a claim of a violation of the Second Amendment is a very close question.

Lack of standing by one plaintiff is not dispositive, however. See *Village of Arlington Heights v. Metro. Hous. Dev. Corp.*, 429 U.S. 252, 264 (1977) (court need not decide third-party standing question, "[f]or we have at least one individual plaintiff who has demonstrated standing to assert these rights as his own"). And SAF's standing presents a much less difficult question. It asserts it has standing, as an association, to assert the rights of its members. See *Warth v.*

⁵ Defense Distributed describes itself as organized and operated "for the purpose of defending the civil liberty of popular access to arms guaranteed by the United States Constitution" through "facilitating global access to" information related to 3D printing of firearms, and specifically "to publish and distribute, *at no cost to the public*, such information and knowledge on the Internet in promotion of the public interest." (Compl. ¶ 1) (emphasis added).

Seldin, 422 U.S. 490, 511 (1975) (“[e]ven in the absence of injury to itself, an association may have standing solely as the representative of its members”). Associational standing requires showing: (1) the association’s members have standing to sue in their own right; (2) the interests at issue are germane to the association’s purpose; and (3) the participation of individual members in the lawsuit is not required. *Ass’n of Am. Physicians & Surgeons, Inc. v. Tex. Med. Bd.*, 627 F.3d 547, 550-51 (5th Cir. 2010) (citing *Hunt v. Wash. St. Apple Adver. Comm’n*, 432 U.S. 333, 343 (1977)). “The first prong requires that at least one member of the association have standing to sue in his or her own right.” *National Rifle Ass’n of Am., Inc. v. Bureau of Alcohol, Tobacco, Firearms, & Explosives*, 700 F.3d 185, 191 (5th Cir. 2012).

Defendants limit their challenge to SAF’s standing solely to whether any of its members have standing to sue in their own right. Specifically, Defendants contend SAF has merely asserted a conjectural injury, by suggesting its members would access computer files in the future. In response, SAF has provided affidavit testimony from two of its members stating they would access the computer files at issue via the Defense Distributed website, study, learn from and share the files, but are unable to do so due to Defendants’ interpretation of the ITAR regulatory scheme. (Plf. Reply Exs. 3-4). This testimony satisfies the “injury in fact” portion of the standing inquiry.

Defendants further contend any injury is not fairly traceable to their conduct. They argue the ITAR does not prevent SAF members in the United States from acquiring the files directly from Defense Distributed. But this argument goes to the burden imposed on SAF members, which is a question aimed at the merits of the claim, not standing. See *Davis v. United States*, 131 S. Ct. 2419, 2434, n.10 (one must not “confus[e] weakness on the merits with absence of Article III standing”). In this case, the inability of SAF members to download the computer files at issue off the Internet is the injury in fact of the SAF members, and is clearly traceable to the conduct of Defendants. The Court therefore finds SAF has standing to assert a claim of a violation of the Second Amendment. See *Nat’l Rifle Ass’n*, 700 F.3d at 192 (NRA had standing, on behalf of its

members under 21, to bring suit challenging laws prohibiting federal firearms licensees from selling handguns to 18-to-20-year-olds); *Ezell v. City of Chicago*, 651 F.3d 684, 696 (7th Cir. 2011) (SAF and Illinois Rifle Association had associational standing to challenge city ordinances requiring one hour of firing range training as prerequisite to lawful gun ownership and prohibiting all firing ranges in city); *Mance v. Holder*, 2015 WL 567302, at *5 (N.D. Tex. Feb. 11, 2015) (non-profit organization dedicated to promoting Second Amendment rights had associational standing to bring action challenging federal regulatory regime as it relates to buying, selling, and transporting of handguns over state lines).

b. Merits

The Second Amendment provides: “A well regulated Militia, being necessary to the security of a free State, the right of the people to keep and bear Arms, shall not be infringed.” U.S. Const. amend. II. The Supreme Court has recognized that the Second Amendment confers an individual right to keep and bear arms. *See District of Columbia v. Heller*, 554 U.S. 570, 595 (2008). The Fifth Circuit uses a two-step inquiry to address claims under the Second Amendment. The first step is to determine whether the challenged law impinges upon a right protected by the Second Amendment—that is, whether the law regulates conduct that falls within the scope of the Second Amendment’s guarantee. The second step is to determine whether to apply intermediate or strict scrutiny to the law, and then to determine whether the law survives the proper level of scrutiny. *Nat’l Rifle Ass’n*, 700 F.3d at 194.

In the first step, the court is to “look to whether the law harmonizes with the historical traditions associated with the Second Amendment guarantee.” *Id.* (citing *Heller*, 554 U.S. at 577-628). Defendants argue at some length that restriction by a sovereign of export of firearms and other weapons has a lengthy historical tradition. Plaintiffs do not contest otherwise. Rather, Plaintiffs contend the conduct regulated here impinges on the ability to manufacture one’s own

firearms, in this case, by way of 3D printing.

While the founding fathers did not have access to such technology,⁶ Plaintiffs maintain the ability to manufacture guns falls within the right to keep and bear arms protected by the Second Amendment. Plaintiffs suggest, at the origins of the United States, blacksmithing and forging would have provided citizens with the ability to create their own firearms, and thus bolster their ability to “keep and bear arms.” While Plaintiffs’ logic is appealing, Plaintiffs do not cite any authority for this proposition, nor has the Court located any. The Court further finds telling that in the Supreme Court’s exhaustive historical analysis set forth in *Heller*, the discussion of the meaning of “keep and bear arms” did not touch in any way on an individual’s right to manufacture or create those arms. The Court is thus reluctant to find the ITAR regulations constitute a burden on the core of the Second Amendment.

The Court will nonetheless presume a Second Amendment right is implicated and proceed with the second step of the inquiry, determining the appropriate level of scrutiny to apply. Plaintiffs assert strict scrutiny is proper here, relying on their contention that a core Second Amendment right is implicated. However, the appropriate level of scrutiny “depends on the nature of the conduct being regulated *and* the degree to which the challenged law burdens the right.” *Nat’l Rifle Ass’n*, 700 F.3d at 195 (emphasis added).

The burden imposed here falls well short of that generally at issue in Second Amendment cases. SAF members are not prevented from “possess[ing] and us[ing] a handgun to defend his or her home and family.” *Id.* at 195 (citations omitted). The Fifth Circuit’s decision in *National Rifle Association* is instructive. At issue was a regulatory scheme which prohibited federally licensed firearms dealers from selling handguns to persons under the age of twenty-one. The court reasoned that only intermediate scrutiny applied for three reasons: (1) an age qualification on

⁶ Nonetheless, “the Second Amendment extends, *prima facie*, to all instruments that constitute bearable arms, even those that were not in existence at the time of the founding.” *Heller*, 554 U.S. at 582.

commercial firearm sales was significantly different from a total prohibition on handgun possession; (2) the age restriction did not strike at the core of the Second Amendment by preventing persons aged eighteen to twenty from possessing and using handguns for home defense because it was not a historical outlier; and (3) the restriction only had temporary effect because the targeted group would eventually age out of the restriction's reach. *Id.* at 205–07. In this case, SAF members are not prohibited from manufacturing their own firearms, nor are they prohibited from keeping and bearing other firearms. Most strikingly, SAF members in the United States are not prohibited from acquiring the computer files at issue directly from Defense Distributed. The Court thus concludes only intermediate scrutiny is warranted here. *See also Nat'l Rifle Ass'n of Am., Inc. v. McCraw*, 719 F.3d 338, 347-48 (5th Cir. 2013), *cert. denied*, 134 S. Ct. 1365 (2014) (applying intermediate scrutiny to constitutional challenge to state statute prohibiting 18-20-year-olds from carrying handguns in public).

As reviewed above, the regulatory scheme of the AECA and ITAR survives an intermediate level of scrutiny, as it advances a legitimate governmental interest in a not unduly burdensome fashion. *See also McCraw*, 719 F.3d at 348 (statute limiting under 21-year-olds from carrying handguns in public advances important government objective of advancing public safety by curbing violent crime); *Nat'l Rifle Ass'n*, 700 F.3d at 209 (“The legitimate and compelling state interest in protecting the community from crime cannot be doubted.”). Accordingly, the Court finds Plaintiffs have not shown a substantial likelihood of success on the merits.

E. Fifth Amendment

Plaintiffs finally argue the prior restraint scheme of the ITAR is void for vagueness and thus in violation of their right to due process. “It is a basic principle of due process that an enactment is void for vagueness if its prohibitions are not clearly defined.” *Grayned v. City of Rockford*, 408 U.S. 104, 108 (1972). The Fifth Amendment prohibits the enforcement of vague criminal laws, but

the threshold for declaring a law void for vagueness is high. “The strong presumptive validity that attaches to an Act of Congress has led this Court to hold many times that statutes are not automatically invalidated as vague simply because difficulty is found in determining whether certain marginal offenses fall within their language.” *United States v. Nat’l Dairy Prods. Corp.*, 372 U.S. 29, 32 (1963). Rather, it is sufficient if a statute sets out an “ascertainable standard.” *United States v. L. Cohen Grocery Co.*, 255 U.S. 81, 89 (1921). A statute is thus void for vagueness only if it wholly “fails to provide a person of ordinary intelligence fair notice of what is prohibited, or is so standardless that it authorizes or encourages seriously discriminatory enforcement.” *United States v. Williams*, 553 U.S. 285, 304 (2008).

Plaintiffs here assert broadly that ITAR is unconstitutionally vague because “persons of ordinary intelligence” must guess as to whether their speech would fall under its auspices. As an initial matter, the Court notes at least two circuits have rejected due process challenges to the AECA and ITAR, and upheld criminal convictions for its violation. See *Zhen Zhou Wu*, 711 F.3d at 13 (rejecting defendants’ argument “that this carefully crafted regulatory scheme—which has remained in place for more than a quarter century—is unconstitutionally vague” as applied to them); *United States v. Hsu*, 364 F.3d 192, 198 (4th Cir. 2004) (holding the AECA and its implementing regulations not unconstitutionally vague as applied to defendants). Plaintiffs neither acknowledge those decisions nor explain how their rationale is inapplicable to their situation.

The Supreme Court has recently noted its precedent generally limits such challenges to “statutes that tied criminal culpability” to conduct which required “wholly subjective judgments without statutory definitions, narrowing context, or settled legal meanings.” *Humanitarian Law Project*, 561 U.S. at 20 (quoting *Williams*, 553 U.S. at 306). Plaintiffs’ challenge here is additionally hampered because they have not made precisely clear which portion of the ITAR language they believe is unconstitutionally vague.

To the degree Plaintiffs contend “defense articles” is vague, as Defendants point out, the

term “defense articles” is specifically defined to include items on the Munitions List, which contains twenty-one categories of governed articles, as well as information “which is required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance or modification of defense articles” which additionally “includes information in the form of blueprints, drawings, photographs, plans, instructions or documentation.” See 22 C.F.R. §§ 120.6 (defining “defense articles”), 120.10 (a) (defining technical data) & 121.1 (Munitions List). Although lengthy, the cited regulations do not themselves include subjective terms, but rather identify items with significant specificity. For example, the first category “Firearms, Close Assault Weapons and Combat Shotguns” includes eight subcategories such as “Nonautomatic and semi-automatic firearms to caliber .50 inclusive (12.7 mm),” as well as six interpretations of the terms. 22 C.F.R. § 121.1. The Court has little trouble finding these provisions survive a vagueness challenge.

The term “export” is also defined in the ITAR, although at lesser length. At issue here, “export” is defined to include “[d]isclosing (including oral or visual disclosure) or transferring technical data to a foreign person, whether in the United States or abroad.” 22 C.F.R. § 120.17(a)(4). Plaintiffs here admit they wish to post on the Internet, for free download, files which include directions for the 3D printing of firearms. Persons of ordinary intelligence are clearly put on notice by the language of the regulations that such a posting would fall within the definition of export.

Accordingly, the Court concludes Plaintiffs have not shown a likelihood of success on the merits of their claim under the Fifth Amendment.

IV. CONCLUSION

Plaintiffs' Motion for Preliminary Injunction (Clerk's Dkt. #7) is hereby **DENIED**.

SIGNED on August 4, 2015.

A handwritten signature in blue ink, appearing to read "R. Pitman", with a long horizontal stroke extending to the right.

ROBERT L. PITMAN
UNITED STATES DISTRICT JUDGE



United States Department of State

*Bureau of Political-Military Affairs
Directorate of Defense Trade Controls*

Washington, D.C. 20522-0112

In Reply refer to
DDTC Cases CJ 651-13 through 660-13

JUN 04 2015

YOUR SUBMISSION DATED: June 21, 2013

COMMODITY JURISDICTION DETERMINATIONS FOR: Liberator Pistol Data Files, .22 Electric Data Files, 125 mm BK-14M High Explosive Anti-Tank Warhead Model Data File, 5.56/.223 Muzzle Brake Data Files, Springfield XD-40 Tactical Slide Assembly Data Files, Sound Moderator - Slip On Data File, "The Dirty Diane" Oil Filter Silencer Adapter Data File, 12 Gauge to .22 CB Sub-Caliber Insert Data Files, Voltlock Electronic Black Powder System Data Files, and VZ-58 Front Sight Data Files

The data described in your submission are Computer Aided Design (CAD) data files that can be used in a 3D printer to produce physical models of the associated item.

A technical review of your commodity jurisdiction (CJ) request has been concluded by requisite agencies of the United States Government. The findings of that technical review are:

The Department of State has determined that the **125 mm BK-14M High Explosive Anti-Tank Warhead Model Data File, Sound Moderator - Slip On Data File, and "The Dirty Diane" Oil Filter Silencer Adapter Data File** are **not subject to the jurisdiction of the Department of State**. The Department of Commerce (DOC) advises that these items are classified as EAR99. Please consult the DOC Office of Exporter Services at (202) 482-4811 to satisfy applicable requirements prior to export.

The Department of State has determined that the **Voltlock Electronic Black Powder System Data Files** are **not subject to the jurisdiction of the**

Continued on Page Two

Cody R. Wilson
Defense Distributed
711 W. 32nd Street, Apt. 115
Austin, TX 78705
crw@defdist.org

Page Two

In Reply refer to
DDTC Cases CJ 651-13 through 660-13

Department of State. However, export may require authorization from the Department of Commerce (DOC). Please consult the DOC Office of Exporter Services at (202) 482-4811 to make a Classification Request (CCATS) and satisfy other applicable requirements prior to export.

The Department of State has determined that the **Liberator Pistol Data Files, .22 Electric Data Files, 5.56/.223 Muzzle Brake Data Files, Springfield XD-40 Tactical Slide Assembly Data Files, 12 Gauge to .22 CB Sub-Caliber Insert Data Files (except for "read me" text file), and VZ-58 Front Sight Data Files** are subject to the jurisdiction of the Department of State in accordance with the **International Traffic in Arms Regulations (ITAR) (22 CFR 120 through 130)**. They are designated as technical data under Category I(i) of the United States Munitions List (USML) pursuant to §120.10 of the ITAR. A license or other approval is required pursuant to the ITAR prior to any export or temporary import.

Should you not concur with this determination and have additional facts not included in the original submission, you may submit a new CJ request. If you do not concur with this determination and have no additional facts to present, then you may request that this determination be reviewed by the Deputy Assistant Secretary of State for Defense Trade Controls.

Should you require further assistance on this matter, please contact Sam Harmon at (202) 663-2811 or HarmonSC@state.gov.

Sincerely,



C. Edward Peartree

Director

Office of Defense Trade Controls Policy

Cc: Matthew A. Goldstein
1012 14th Street, NW, Suite 620
Washington, DC 20005
matthew@goldsteinpllc.com



United States Department of State

*Bureau of Political-Military Affairs
Directorate of Defense Trade Controls
Washington, D.C. 20522-0112*

In Reply refer to
DDTC Case CJ 1083-14

APR 13 2015

YOUR SUBMISSION DATED: January 2, 2015

COMMODITY JURISDICTION DETERMINATION FOR: Ghost Gunner Machine, Plastic Mounting Jig, User Instructions, and Software

The product described in your submission is a one cubic foot box that functions as a 3-axis, computer-numerically-controlled (CNC) press capable of automatically milling parts out of various materials through user-provided software designs.

A technical review of your commodity jurisdiction (CJ) request has been concluded by the requisite agencies of the United States Government. A split jurisdiction determination of this request has been determined, as follows:

The Department of State has determined that the **Ghost Gunner Machine, Plastic Mounting Jig, and User Instructions are not subject to the jurisdiction of the Department of State.** However, export may require authorization from the Department of Commerce (DOC). Please consult the DOC Office of Exporter Services at (202) 482-4811 to make a Classification Request (CCATS) and satisfy other applicable requirements prior to export.

The Department of State has determined that the **software, data files, project files, coding, and models for producing a defense article, to include 80% AR-15 lower receivers, are subject to the jurisdiction of the Department of State in accordance with the International Traffic in Arms Regulations (ITAR) (22 CFR 120 through 130).** They are designated as technical

Continued on Page Two

Cody R. Wilson
Defense Distributed, Inc.
1101 W 34th Street, #340
Austin, TX 78705
crw@defdist.org
DOSWASHINGTONSUP00568

Page Two


In Reply refer to
DDTC Case CJ 1083-14

data under Category I(i) of the United States Munitions List (USML). A license or other approval is required pursuant to the ITAR prior to any export or temporary import.

Should you not agree with this determination and have additional facts not included in the original submission, you may submit a new CJ request. If you do not agree with this determination and have no additional facts to present, you may request that this determination be reviewed by the Deputy Assistant Secretary of State for Defense Trade Controls.

Should you require further assistance on this matter, please contact Kylie Gaskins at (202) 663-2825 or GaskinsKJ@state.gov.

Sincerely,



C. Edward Peartree

Director

Office of Defense Trade Controls Policy

Cc: Matthew A. Goldstein
1012 14th Street, NW, Suite 620
Washington, DC 20005
matthew@goldsteinpllc.com